WITTS SATZ FÜR SEMILOKALE RINGE

Dissertation
zur Erlangung des Doktorgrades
der Mathematisch-Naturwissenschaftlichen Fakultät
der Georg-August-Universität zu Göttingen

vorgelegt von

HANS REITER

aus Wien

Mainz 1973

Digitized by the Internet Archive
in 2026

https://archive.org/details/IA41534919_0010

Druck- und Verlagsanstalt

Werner Blasaditsch · 89 Augsburg · Theodor-Heuss-Platz 3 · Telefon (0821) 25563

Printed in Germany

Witts Satz für semilokale Ringe

DISSERTATION

zur Erlangung des Doktorgrades

der Mathematisch- Naturwissenschaftlichen Fakultät

der Georg-August-Universität zu Göttingen

vorgelegt von

HANS REITER

aus Wien

Mainz 1972

UNIV.
LEIDEN
BIBL.

D 7

Referent: Prof. Dr. M. Kneser

Korreferent: Prof. Dr. M. Deuring

Tag der mündlichen Prüfung: 15.2.1973

Inhaltsverzeichnis

	Seite
Einleitung	1
§1 Quadratische Formen über Ringen und Spiegelungen	3
§2 Quadratische Moduln über halbeinfachen Ringen	11
§3 Hilfssätze	16
§4 Witts Satz für Schiefkörper und Summen zweier Schiefkörper	27
§5 Witts Satz für halbeinfache Ringe	33
§6 Witts Satz für semilokale Ringe	36
Literaturverzeichnis	44

Einleitung

Diese Arbeit beschäftigt sich mit der Frage, inwiefern man Witts Satz über die Fortsetzbarkeit von Isometrien quadratischer Moduln unter den Voraussetzungen, die M.Kneser in -5- für kommutative lokale Ringe macht, auch für nicht notwendig kommutative semilokale Ringe beweisen kann. Dazu brauchen wir eine Erweiterung des Begriffs "quadratischer Modul" auf nichtkommutative Ringe. Die allgemeinste für uns brauchbare Definition findet sich bei C.T.C.Wall in -6-. In §1 stellen wir das zusammen, was wir aus dieser Arbeit übernehmen und zeigen, daß es auf diesen Moduln Isometrien gibt, die ähnliche Eigenschaften haben wie die Spiegelungen im klassischen Fall und die wir deshalb ebenfalls "Spiegelungen" nennen. Auch §2 ist noch von vorbereitender Natur und in §3 beweisen wir Hilfssätze, die wir für das Folgende benötigen. In den Paragraphen 4,5 und 6 folgt dann "Witts Satz" unter immer schwächer werdenden Bedingungen an den Ring A. Von einigen Ausnahmefällen abgesehen erhalten wir stets das folgende Ergebnis:

> Sind F und G freie Untermoduln endlicher Dimension eines quadratischen Moduls E, $t: F \to G$ eine Isometrie und gibt es einen Untermodul H von E derart, daß für Basen $\{f_i\}$ von F und $\{g_i\}$ von G Elemente $h_i, h_i' \in H$ existieren mit $b(f_i, h_j) = \delta_{ij}$, $b(g_i, h_j') = \delta_{ij}$, so gibt es ein Produkt von Spiegelungen bezüglich Elementen aus H, das t zu einer Isometrie von E fortsetzt.

§4 behandelt den Fall von Schiefkörpern mit Involution oder Summen zweier Schiefkörper, die durch eine Involution vertauscht werden.

Den Beweis dieses Satzes führen wir im Wesentlichen wie in -5- Satz 1, und aus unserem Ergebnis kann man leicht das dortige bekommen. In §5 beweisen wir den analogen Satz für halbeinfache Ringe. Das Resultat, das wir in Satz 5.1 erhalten, verallgemeinert das von McEvett aus -3- Chapter 3. §6 schließlich behandelt den Fall eines (nicht notwendig kommutativen) semilokalen Ringes. Hier zeigen wir in Satz 6.3 noch, daß einige Ausnahmefälle wegfallen und daß der Satz auch für endlich erzeugte projektive Moduln F und G gilt, falls wir nicht fordern, daß die Isometrie von E, die $t: F \to G$ fortsetzt, ein Produkt von Spiegelungen ist. Für kommutative semilokale Ringe ist dies Problem bereits von M.Knebusch in -4- behandelt worden und ein Teil seiner Resultate folgt auch aus dem hier bewiesenen.

§1 Quadratische Formen über Ringen und Spiegelungen.

Die folgenden Bezeichnungen und Definitionen gelten für die ganze Arbeit:

A ist ein Ring mit Einselement und A^* die Einheitengruppe von A,

α ein Antiautomorphismus von A für den es ein $u \in A^*$ gibt mit:

1.1 $\alpha(u) = u^{-1}$ und

1.2 $\alpha^2(a) = uau^{-1}$ für alle $a \in A$.

E ist ein unitärer A-Rechtsmodul und

$\Phi: E \times E \to A$ eine α-Sesquilinearform. Ferner

$S_\alpha(E) = \{ \Phi \mid \Phi: E \times E \to A$ ist α-Sesquilinearform $\}$ mit der Gruppenstruktur, die man durch

$(\Phi_1 + \Phi_2)(x,y) = \Phi_1(x,y) + \Phi_2(x,y)$ für alle $\Phi_1, \Phi_2 \in S_\alpha(E)$, $x,y \in E$ erhält und

$T_u: S_\alpha(E) \to S_\alpha(E)$ der Gruppenhomomorphismus, der gegeben ist durch $T_u(\Phi)(x,y) = \alpha(\Phi(y,x))u$. Es gilt: $T_u^2 = 1$, wobei 1 die Identität auf $S_\alpha(E)$ bezeichnet. Wir setzen:

$R_{\alpha,u}(E) = \mathrm{Kern}(T_u - 1)$ und $Q_{\alpha,u}(E) = \mathrm{Cokern}(T_u - 1)$. Wegen $T_u^2 - 1 = 0$ liefert $T_u + 1$ eine Abbildung

$b: Q_{\alpha,u}(E) \to R_{\alpha,u}(E)$. Sei b_Θ das Bild von $\Theta \in Q_{\alpha,u}(E)$ unter b.

$A(\alpha,u) = \{ a - \alpha(a)u \mid a \in A \}$ sei die additive Untergruppe der α,u-alternierenden Elemente von A.

Ist $\Theta \in Q_{\alpha,u}(E)$ und sind Φ, Φ' Vertreter von Θ in $S_\alpha(E)$, so gilt $(\Phi' - \Phi)(x,x) \in A(\alpha,u)$ für alle $x \in E$. Durch $q_\Theta(x) = \Phi(x,x) + A(\alpha,u)$ erhalten wir also eine Abbildung $q_\Theta: E \to A/A(\alpha,u)$. Ist r ein Vertreter von $q_\Theta(x)$ in A, so hängen für $a \in A$

$\alpha(a)q_\Theta(x)a = \alpha(a)ra + A(\alpha,u) \in A/A(\alpha,u)$ und

$q_\Theta(x) + \alpha(q_\Theta(x))u = r + \alpha(r)u \in A$ nicht von der Auswahl des Vertreters r ab, so daß wir folgende Rechenregeln haben:

1.3 $q_\Theta(x + y) - q_\Theta(x) - q_\Theta(y) = b_\Theta(x,y) + A(\alpha,u)$,

1.4 $q_\Theta(xa) = \alpha(a)q_\Theta(x)a$ und

1.5 $q_\Theta(x) + \alpha(q_\Theta(x))u = b_\Theta(x,x)$ für alle $x,y \in E$, $a \in A$.

Damit haben wir jedem $\Theta \in Q_{\alpha,u}(E)$ ein Paar b_Θ, q_Θ zugeordnet, so daß 1.3-1.5 gelten. Bezeichnen wir mit $Quad_{\alpha,u}(E)$ die Menge aller Paare b,q mit $b \in R_{\alpha,u}(E)$, $q: E \to A/A(\alpha,u)$ für die 1.3-1.5 erfüllt sind, so erhalten wir eine Abbildung

1.6 $Q_{\alpha,u}(E) \to Quad_{\alpha,u}(E)$ durch $\Theta \to b_\Theta, q_\Theta$.

1.7 SATZ Ist E projektiv, so ist die Abbildung aus 1.6 bijektiv.

Ein Beweis dieses Satzes steht in -6- Theorem 1.

Im Allgemeinen haben wir nun zwei Möglichkeiten, Formen auf einem Modul E zu definieren. Wir werden in beiden Fällen von quadratischen Formen sprechen und das Paar E,Θ bzw. das Tripel E,b,q einen quadratischen α,u-Modul nennen. In naheliegender Weise definieren wir die orthogonale Summe zweier quadratischer α,u-Moduln und den Orthogonalraum $F^\perp$ eines Untermoduls F von E bezüglich b_Θ bzw. b. Unter einer Isometrie s zwischen zwei quadratischen α,u-Moduln E,Θ und E',Θ' verstehen wir einen Modulisomorphismus für den zusätzlich gilt:

$\Phi'(s \times s) - \Phi \in (T_u - 1)S_\alpha(E)$, wobei Φ ein Vertreter von Θ in $S_\alpha(E)$, Φ' einer von Θ' in $S_\alpha(E')$ ist und wobei

$\Phi'(s \times s)(x,y) = \Phi'(s(x),s(y))$ für alle $x,y \in E$ gilt.

Sind quadratische α,u-Moduln E,b,q und E',b',q' gegeben, so sei s ein Modulisomorphismus mit $b'(s(x),s(y)) = b(x,y)$ und $q'(s(x)) = q(x)$ für alle $x,y \in E$.

Wir werden im folgenden hauptsächlich Isometrien der Form $s: x \to x - hl(x)$ $x \in E$ betrachten, wobei $h \in E$ und $l \in \mathrm{Hom}(E,A)$ ist, und wir sind an möglichst vielen solchen Isometrien interessiert. Um diese zu definieren brauchen wir eine Vorbemerkung. Sei $e \neq 0$ ein Idempotent in A mit $\alpha(e) = e$. Dann gilt: $eAe = R$ ist ein Ring mit Einselement e und $\alpha(R) = R$. Ist $ue = eu$, so folgt: $R(\alpha,eue) = \{ r - \alpha(r)eue \mid r \in R \} = eA(\alpha,u)e$, wie man sofort nachrechnet. Ist $c \in R^*$, so bezeichnen wir mit c_R^{-1} das Inverse von c in R und betrachten es auch als Element von A. Wir können nun definieren:

1.8 DEFINITION Sei E,Θ bzw. E,b,q ein quadratischer α,u-Modul, $e \neq 0$ ein Idempotent in A mit $\alpha(e) = e$ sowie $ue = eu$ und sei auch im Fall E,Θ b,q anstelle von b_Θ, q_Θ gesetzt. Ferner sei $h \in E$ so, daß für einen Vertreter $c \in R$ von $eq(h)e = q(he)$ gilt $c \in R^*$. Dann heißt $s_{h,e,c}: x \to x - hec_R^{-1}b(h,x)$ $(x \in E)$ eine e-Spiegelung bezüglich h,c.

Ist $e = 1$, so schreiben wir $s_{h,c}$ anstelle von $s_{h,1,c}$ und nennen $s_{h,c}$ eine Spiegelung.

Ist E,Θ ein quadratischer α,u-Modul, Φ ein Vertreter von Θ in $S_\alpha(E)$, so war $q_\Theta(x) = \Phi(x,x) + A(\alpha,u)$. Für jeden Vertreter c von $eq_\Theta(x)e$ in R gibt es also ein $t \in A$ mit $e\Phi(x,x)e + t - \alpha(t)u = c \in R$. Es folgt: $c = ece = e(\Phi(x,x) + t - \alpha(t)u)e$. Nach dieser Bemerkung wollen wir nun beweisen, daß für e-Spiegelungen gilt:

1.9 SATZ $s_{h,e,c}$ ist eine Isometrie mit Inversem $s_{h,e,\alpha(c)u}$

BEWEIS: $s_{h,e,c}$ ist eine A-lineare Abbildung, da b_θ bzw. b rechtslinear ist. Wir zeigen nun, daß $s_{h,e,c}$ mit θ verträglich ist. Ist $\Phi\varepsilon S_\alpha(E)$ ein fester Vertreter von θ und $t\varepsilon A$ so, daß $e(\Phi(h,h) + t - \alpha(t)u)e = c\varepsilon R^*$ ist, so müssen wir zeigen: Für alle $\chi\varepsilon S_\alpha(E)$ gibt es ein $\Psi\varepsilon S_\alpha(E)$ mit:

$(\Phi + (T_u - 1_{S_\alpha(E)})\chi)(s_{h,e,c}(x),s_{h,e,c}(y)) =$

$(\Phi + (T_u - 1_{S_\alpha(E)})\Psi)(x,y)$ für alle $x,y\varepsilon E$.

Es gilt: $s_{h,e,c}(x) = x - hec_R^{-1}b_\theta(h,x)$. Sei $l(x) = c_R^{-1}b_\theta(h,x)$.

Dann folgt: $\Phi(s_{h,e,c}(x),s_{h,e,c}(y)) - \Phi(x,y) =$

$\alpha(l(x))(e\Phi(h,h)el(y) - e\Phi(h,y)) - \Phi(x,h)el(y) =$

$\alpha(l(x))((c + e(\alpha(t)u - t)e)l(y) - e\Phi(h,y)) - \Phi(x,h)el(y) =$

$\alpha(l(x))(eb_\theta(h,y) - e\Phi(h,y) + e(\alpha(t)u - t)el(y)) -$

$\Phi(x,h)el(y) =$

$\alpha(l(x))e(\alpha(\Phi(y,h))u + \alpha(t)uel(y)) - (\Phi(x,h) + \alpha(l(x))et)el(y)$

Sei $\Psi_o(x,y) = (\Phi(x,h) + \alpha(l(x))et)el(y)$. Es folgt:

$T_u(\Psi_o)(x,y) = \alpha(l(x))e(\alpha(\Phi(y,h) + \alpha(t)eul(y)u^{-1})u$

$= \alpha(l(x))e(\alpha(\Phi(y,h)u + \alpha(t)uel(y))$

Ferner $\Psi_1(x,y) = \chi(s_{h,e,c}(x),s_{h,e,c}(y))$. Mit $\Psi = \Psi_o + \Psi_1$ erhält man dann die Behauptung.

Im Fall eines quadratischen α,u-Moduls E,b,q ist zu zeigen:

$q(s_{h,e,c}(x)) = q(x)$ und $b(s_{h,e,c}(x),s_{h,e,c}(y)) = b(x,y)$

für alle $x,y\varepsilon E$. Es ist, wenn man $l(x) = c_R^{-1}b(h,x)$ setzt:

$q(s_{h,e,c}(x)) - q(x) =$

$\alpha(l(x))eq(h)el(x) - (\alpha(l(x))eb(h,x) + A(\alpha,u)) =$

$\alpha(l(x))(cl(x) - eb(h,x)) + A(\alpha,u) = A(\alpha,u)$

$b(s_{h,e,c}(x),s_{h,e,c}(y)) - b(x,y) =$

$\alpha(l(x))(eb(h,h)el(y) - eb(h,y)) - b(x,h)el(y) =$

$\alpha(l(x))((c + \alpha(c)u)l(y) - eb(h,y)) - b(x,h)el(y) =$

$(\alpha(l(x))\alpha(c)u - b(x,h)e)l(y) =$

$(\alpha(eb(h,x))u - b(x,h)e)l(y) = 0$, da $\alpha(b(h,x))u = b(x,h)$ ist.

Es bleibt zu zeigen: $\alpha(c)u\varepsilon R^*$ und $s_{h,e,c}s_{h,e,\alpha(c)u} = 1_E$.

$s_{h,e,\alpha(c)u}s_{h,e,c} = 1_E$ folgt dann wegen $\alpha(\alpha(c)u)u = c$.

Es ist $\alpha(c)u = (\alpha(c)e^2)u = \alpha(c)(eue)\varepsilon R^*$. Ferner für einen Modul b,q,E und mit b_Θ anstelle von b im anderen Fall:

$s_{h,e,c}s_{h,e,\alpha(c)u}(x) = s_{h,e,c}(x - he(\alpha(c)u)_R^{-1}b(h,x)) =$

$x - he(c_R^{-1} + (\alpha(c)u)_R^{-1} - (c_R^{-1}e)b(h,h)e(\alpha(c)u)_R^{-1})b(h,x) =$

$x - he(c_R^{-1} + (\alpha(c)u)_R^{-1} - c_R^{-1}(c + \alpha(c)u)(\alpha(c)u)_R^{-1})b(h,x) = x.$

1.10 SPEZIALFALL Sind $x,y\varepsilon E$ mit $q_\Theta(x) = q_\Theta(y)$ und $b_\Theta(x - y,x)\varepsilon A^*$ bzw. $q(x) = q(y)$ und $b(x - y,x)\varepsilon A^*$, so gibt es eine Spiegelung $s_{h,c}$ mit $s_{h,c}(x) = y$.

BEWEIS Sei $h = x - y$, $\Phi\varepsilon S_\alpha(E)$ ein Vertreter von Θ. Es gilt

$\Phi(y,y) = \Phi(x,x) + t_o - \alpha(t_o)u$, da $q_\Theta(x) = q_\Theta(y)$ ist und damit folgt: $\Phi(h,h) - b_\Theta(x - y,x) =$

$\Phi(x - y,x) - \Phi(x,y) + \Phi(y,y) - \Phi(x - y,x) - \alpha(\Phi(x,x - y))u$

$= (\Phi(x,x - y) + t_o) - \alpha(\Phi(x,x - y) + t_o)u$. Für

$t = -(\Phi(x,x - y) + t_o)$ gilt also

$\Phi(h,h) + t - \alpha(t)u = b_\Theta(x - y,x)\varepsilon A^*$ und man erhält:

$s_{h,b_\Theta(x - y,x)}(x) = x - h = y.$

Im anderen Fall ist ebenso $b(h,x)$ ein Vertreter von $q(h)$ in A^* und es gilt $s_{h,b(h,x)}(x) = x - h = y$.

1.11 SPEZIALFALL Sind $x,y \in E$ mit $q(x) = q(y)$ und $h \in E$ so, daß für ein $c \in A^*$ die Spiegelung $s_{h,c}$ existiert und so, daß $b(y,h') \in A^*$ ist, wobei gilt:

$h' = y - x + hc^{-1}b(h,x)$, so folgt:

$s_{h',b(y,h')}s_{h,c}(x) = y$.

Dieser Spezialfall ist insbesondere immer dann erfüllt, wenn $b(y,y - x) = 0$ ist und $b(y,h)$ sowie $b(x,h)$ Einheiten in A sind.

Entsprechendes hat man für b_Θ, q_Θ anstelle von b,q für den Fall eines Moduls E,Θ.

BEWEIS Es ist zunächst zu zeigen, daß $b(y,h') \in q(h')$ ist bzw., daß es ein $t \in A$ gibt mit $\Phi(h',h') + t - \alpha(t)u = b_\Theta(y,h')$, wobei Φ ein Vertreter von Θ in $S_\alpha(E)$ ist. Es gilt:

$q(y) = q(x) = q(s_{h,c}(x)) = q(x - hc^{-1}b(h,x)) = q(y - h')$

$= q(y) + q(h') - (b(y,h') + A(\alpha,u))$, also:

$b(y,h') \in q(h')$. Ebenso:

$b_\Theta(y,h') \in q_\Theta(h')$ Da Φ ein Vertreter von Θ in $S_\alpha(E)$ ist, folgt: $b_\Theta(y,h') = \Phi(h',h') + t - \alpha(t)u$ für ein $t \in A$. Es gilt:

$b(h',h') = q(h') + \alpha(q(h'))u = b(y,h') + b(h',y)$, also:

$b(h',y - h') = -b(y,h')$. Dies liefert:

$s_{h',b(y,h')}s_{h,c}(x) = s_{h',b(y,h')}(x - hc^{-1}b(h,x)) =$

$s_{h',b(y,h')}(y - h') = y - h' - h'b(y,h')^{-1}b(h',y - h') = y$.

Ist $b(y,y - x) = 0$, $b(y,h), b(x,h) \in A^*$, so folgt:

$b(y,h') = b(y,y - x) + b(y,h)c^{-1}b(h,x) \in A^*$, denn mit $b(x,h)$ ist auch $b(h,x) = \alpha(b(x,h))u \in A^*$. Dies alles geht ebenso für b_Θ, q_Θ anstelle von b,q.

Ist $e \in A$ wieder ein Idempotent mit $\alpha(e) = e$, $eu = ue$ und $R = eAe$, so ist $R(\alpha,eue) = eA(\alpha,u)e = R \cap A(\alpha,u)$. Wir setzen $E_R = Ee$ und $\pi(x) = xe$ für $x \in E$. E_R ist ein R-Modul, da für $r \in R$ gilt: $er = re$, und π ist ein R-Modulhomomorphismus. Ist für einen Vertreter Φ von Θ in $S_\alpha(E)$ $\Phi_R = \Phi|_{S_\alpha(E_R)}$, so erhalten wir durch $\Theta_R = \Phi_R + (T_{eue} - 1)S_\alpha(E_R)$ einen quadratischen α,eue-Modul E_R,Θ_R, wie man unmittelbar nachrechnet. Ebenso ist für $b,q \in Quad_{\alpha,u}(E)$ $b_R = b|_{E_R \times E_R} \in R_{\alpha,eue}(E_R)$ und für $x \in E_R$ gilt $eq(x)e = q(x)$, also gibt es einen mod $R(\alpha,eue)$ eindeutig bestimmten Vertreter r von $q(x)$ in R. Sei $q_R(x) = r + R(\alpha,eue) \in R/R(\alpha,eue)$. q_R erfüllt wieder 1.3-1.5, wir haben also jedem quadratischen α,u-Modul über A einen quadratischen α,eue-Modul über R zugeordnet. Dafür gilt nun:

1.12 SATZ Existiert $s_{\pi(h),c}: E_R \to E_R$, so auch $s_{h,e,c}: E \to E$ und umgekehrt und es gilt für alle $x \in E$:

$$s_{\pi(h),c}(\pi(x)) = \pi(s_{h,e,c}(x)).$$

Ist $F \subseteq E$ ein Untermodul, $t: F \to E$ A-linear, so ist $t_R: \pi(F) \to \pi(E)$ mit $t_R(\pi(f)) = \pi(t(f))$ für alle $f \in F$ eine R-lineare Abbildung. Ist G ein weiterer Untermodul von E, $t: F \to G$ eine Isometrie, so auch $t_R: \pi(F) \to \pi(G)$.

BEWEIS Für alle $x \in E$ gilt: $\pi(s_{h,e,c}(x)) = \pi(x - hec_R^{-1}b(h,x)) = \pi(x) - \pi(h)c_R^{-1}b(\pi(h),\pi(x)) = s_{\pi(h),c}(\pi(x))$.

Gilt $\pi(f) = \pi(f')$, so folgt: $\pi(t(f)) = t(fe) = t(f'e) = \pi(t(f'))$, also ist t_R wohldefiniert, und es ist R-linear, da für $r \in R$ $er = re$ ist. Gilt $\Phi(t \times t) - \Phi \in (T_u - 1)S_\alpha(F)$ für einen Vertreter Φ von Θ in $S_\alpha(E)$, so rechnet man nach: $\Phi_R(t_R \times t_R) - \Phi_R \in (T_{eue} - 1)S_\alpha(\pi(F))$; Analoges gilt für

b und q. Ferner induziert t^{-1}: G → F eine Abbildung $(t^{-1})_R$ und es gilt offensichtlich $(t^{-1})_R = (t_R)^{-1}$.

Die folgende Behauptung kann man unmittelbar nachrechnen, sie findet sich zum Teil auch in -6-.

1.13 LEMMA: Hat man auf A zwei Antiautomorphismen α,β, für die es ein $v\in A^*$ gibt mit $\beta(a) = v^{-1}\alpha(a)v$ für alle $a\in A$, so können wir einem quadratischen α,u-Modul E,Θ einen quadratischen $\beta,v^{-1}\alpha(v)u$-Modul $E,v^{-1}\Theta$ zuordnen durch: $(v^{-1}\Phi)(x,y) = v^{-1}\Phi(x,y)$ für einen Vertreter Φ von Θ in $S_\alpha(E)$ und alle $x,y\in E$; analog einem quadratischen α,u-Modul E,b,q einen quadratischen $\beta,v^{-1}\alpha(v)u$-Modul $E,v^{-1}b,v^{-1}q$. Die Isometrien sowie die Spiegelungen von E,Θ und $E,v^{-1}\Theta$ bzw. E,b,q und $E,v^{-1}b,v^{-1}q$ entsprechen sich umkehrbar eindeutig.

§2 Quadratische Moduln über halbeinfachen Ringen.

Wir betrachten im Folgenden halbeinfache Ringe A, die einen Antiautomorphismus α und ein $u \in A^*$ besitzen, so daß 1.1 und 1.2 erfüllt sind. Da α^2 ein innerer Automorphismus ist, führt α^2 jede Komponente der Zerlegung von A in einfache Ringe in sich über. Außerdem ist das Bild eines einfachen Ringes unter α wieder einfach, also vertauscht α entweder zwei der obigen Komponenten oder führt eine solche schon in sich über. Durch direkte Zerlegung von A und entsprechende Zerlegung der quadratischen Moduln können wir uns also auf die Fälle beschränken, daß A entweder einfach oder eine direkte Summe zweier einfacher Ringe A_1 und $A_2 = \alpha(A_1)$ ist. Nach -2- §5.4 Théorème 2 gilt $A_1 \cong M_n(D)$, dem Ring der n×n-Matrizen über einem Schiefkörper D. Seien e_{ij} die Matrizen aus $M_n(D)$, die an der Stelle i,j eine Eins, sonst überall Null haben und sei D mit $D1_n$ (1_n das Einselement in $M_n(D)$) identifiziert. Setzen wir $\alpha(e_{ij}) = e'_{ji} \in A_2$ und $\alpha(d) = d^{op}$ für $d \in D$, so erhalten wir, daß $A_2 \cong M_n(D^{op})$ ist, wobei D^{op} den zu D oponierten Schiefkörper bezeichnet. Wir können uns also für A auf die folgenden Fälle beschränken:

2.1 $A \cong M_n(D)$ oder

2.2 $A \cong M_n(D) \oplus M_n(D^{op}) \cong M_n(D \oplus D^{op})$ mit

$\alpha((e_{ij},0)) = (0,e'_{ji})$ für $i,j=1,..,n$ und

$\alpha((d,0)) = (0,d^{op})$ für $d \in D$.

Wir bezeichnen im Folgenden mit K das Zentrum von D und schreiben in beiden Fällen $A = M_n(R)$. Dabei ist also $R \cong D$ im Fall 2.1 und $R \cong D \oplus D^{op}$ im Fall 2.2. Es gilt:

2.3 SATZ Es gibt ein $v \in A^*$ derart, daß $\beta: a \to v^{-1}\alpha(a)v$ $(a \in A)$ eine Involution von A ist für die gilt:

2.3.1 $\beta(R) = R$ und $\beta(e_{ij}) = e_{ji}$ für alle $i,j = 1,..,n$

2.3.2 $v^{-1}A(\alpha,u) = A(\beta,\kappa)$ mit $\kappa \in \{\pm 1\}$.

BEWEIS Wir behandeln zunächst den Fall 2.2 und setzen:

$u = (u_1, u_2^{op})$, $v = (u_1, 1)$ und $e_{ij} = (e'_{ij}, e''_{ij})$. Es folgt:

$(u_1^{-1}, (u_2^{op})^{-1}) = u^{-1} = \alpha(u) = (\alpha(u_2^{op}), \alpha(u_1))$ und damit:

$v^{-1}\alpha(v)u = (u_1^{-1}, 1)(1, \alpha(u_1))(u_1, u_2^{op}) = 1$, also ist nach 1.13 $\kappa = 1$ und β eine Involution. Ferner gilt:

$\alpha((0, e''_{ij})) = \alpha^2((e'_{ji}, 0)) = (u_1 e'_{ji} u_1^{-1}, 0)$ also: $\beta(e_{ij}) = e_{ji}$ und für alle $r \in R$ folgt ebenso: $\beta(r) \in R$.

Sei nun $R = D$ und $B = M_n(K)$. Wir betrachten zwei K-Algebrenmonomorphismen ι, λ von B in A, und zwar sei ι die kanonische Einbettung und λ sei definiert durch:

$\lambda(e_{ij}) = \alpha(e_{ji})$ für $i,j = 1,..,n$ und K-lineare Fortsetzung.

Wegen $\lambda(e_{ij})\lambda(e_{kl}) = \alpha(e_{lk}e_{ji}) = \delta_{jk}\alpha(e_{li}) = \lambda(e_{ij}e_{kl})$ ist λ tatsächlich ein K-Algebrenmonomorphismus. Nach dem Satz von SKOLEM-NOETHER (siehe -2- §10.1 Théorème 1) gibt es ein $w \in A^*$ mit $\lambda(b) = w\iota(b)w^{-1}$ für alle $b \in B$. Es folgt:

$\alpha(e_{ij}) = \lambda(e_{ji}) = we_{ji}w^{-1}$ und damit

$ue_{ij}u^{-1} = \alpha^2(e_{ij}) = \alpha(w^{-1})we_{ij}w^{-1}\alpha(w)$ für alle $i,j = 1,..,n$.

$w^{-1}\alpha(w)u$ muß also mit $M_n(K) \subseteq A$ vertauschbar sein und deshalb gilt: $w^{-1}\alpha(w)u = d \in D^*$.

Ist $d = -1$, so setzen wir $v = w$ und erhalten nach 1.13 $\kappa = -1$.

Ist $d \neq -1$, also $1 + d \in A^*$, so setzen wir

$v = w + \alpha(w)u = w(1 + d) \in A^*$ und erhalten nach 1.13:

$\kappa = v^{-1}\alpha(v)u = (w + \alpha(w)u)^{-1}(\alpha(w) + wu^{-1})u = 1$.

In beiden Fällen ist β eine Involution und es gilt: $ve_{ji}v^{-1} = we_{ji}w^{-1} = \alpha(e_{ij})$, also $\beta(e_{ij}) = e_{ji}$, denn im zweiten Fall ist $(1 + d)e_{ji}(1 + d)^{-1} = e_{ji}$. Für alle $d \in D$, $i,j = 1,..,n$ erhalten wir wegen $de_{ij} = e_{ij}d$ auch $d\beta(e_{ji}) = \beta(e_{ji})d$ und daraus $e_{ij}\beta(d) = \beta(d)e_{ij}$. $\beta(d)$ ist also mit $M_n(K)$ vertauschbar, folglich ist auch $\beta(D) = D$.

Aus 1.13 und 2.3 folgt nun, daß wir uns bei der Untersuchung der Isometrien eines quadratischen α,u-Moduls auf den Fall eines quadratischen β,κ-Moduls beschränken können, wobei β eine Involution von A ist mit 2.3.1 und $\kappa \in \{\pm 1\}$. Wir betrachten von nun an allgemeiner irgend einen Ring R mit Involution β und $A = M_n(R)$ mit der Involution $\beta: \sum_{i,j=1}^{n} r_{ij}e_{ij} \to \sum_{i,j=1}^{n} \beta(r_{ji})e_{ij}$ sowie quadratische β,κ-Moduln über A mit $\kappa \in \{\pm 1\}$.

Setzen wir $e = e_{11}$, so gilt $e\kappa = \kappa e$ und $\beta(e) = e$, es gibt also in quadratischen β,κ-Moduln e-Spiegelungen. Außerdem ist $eAe \cong R$, so daß wir die Bezeichnungen aus §1 übernehmen können. Für die in 1.12 eingeführten Moduln E_R, Θ_R bzw. E_R, b_R, q_R gilt nun mit den dortigen Bezeichnungen und $e = e_{11}$:

2.4 SATZ Ist F ein freier Untermodul von E, $f_1,..,f_r$ eine A-Basis von F, F' der von den $f_i e_{j1}$ $i=1,..,r$ $j=1,..,n$ erzeugte R-Modul, so ist F' frei und $\pi|_{F'}$ ist ein R-Modulisomorphismus von F' auf $\pi(F)$. Sind $x,y \in E$ mit $\pi(xe_{j1}) = \pi(ye_{j1})$ für alle $j=1,..,n$, so ist $x = y$.

BEWEIS Offensichtlich ist F' ein freier R-Modul und π ein Monomorphismus. Für $f \in F$ gilt:

$f = \sum_{i=1}^{r} f_i(\sum_{j,k=1}^{n} r_{jk}e_{jk})$ und damit:

$\pi(f) = \sum_{i=1}^{r} f_i \sum_{j=1}^{n} r_{j1}e_{j1} = \sum_{i=1}^{r} \sum_{j=1}^{n} (f_i e_{j1})r_{j1}$ also läßt sich

für jedes $f\varepsilon F$ der Vektor $\pi(f)$ als R-Linearkombination der $f_i e_{j1}$ schreiben. $\pi(xe_{j1}) = \pi(ye_{j1})$ heißt $xe_{j1} = ye_{j1}$. Damit wird $xe_{jj} = xe_{j1}e_{1j} = ye_{j1}e_{1j} = ye_{jj}$ für alle $j=1,..,n$ und $x = \sum_{j=1}^{n} xe_{jj} = \sum_{j=1}^{n} ye_{jj} = y$.

Wir wollen nun noch sehen, wie in diesem Fall e-Spiegelungen und Spiegelungen zusammenhängen. Es gilt:

2.5 SATZ Sei E,Θ bzw. E,b,q ein quadratischer β,κ-Modul, $e = e_{11}$. Seien $h_1,h_2\varepsilon E$ so, daß es Vertreter $c_i\varepsilon R^*$ von $q_\Theta(h_i e)$ bzw. $q(h_i e)$ $(i=1,2)$ gibt.

2.5.1 Ist n ungerade, so gilt $s_{h_1,e,c_1} = s_{h_1 e,C}$ mit

$C = c_1 + t - \beta(t)\kappa$ und $t = \sum_{j=1}^{\frac{n-1}{2}} e_{2j\ 2j+1}$.

2.5.2 Ist n gerade, so gilt: $s_{h_2,e,c_2}s_{h_1,e,c_1} = s_{h_1 e+h_2 e_{12},C}$

mit $C = c_1 + e_{21}b_\Theta(h_2,h_1)e + e_{21}c_2e_{12} + t - \beta(t)\kappa$ und

$t = \sum_{j=2}^{\frac{n}{2}} e_{2j-1\ 2j}$ und ebenso mit b anstelle von b_Θ im Fall eines Moduls E,b,q.

BEWEIS Sei stets Φ ein fester Vertreter von Θ in $S_\beta(E)$. Dann gibt es $t_i\varepsilon A$ mit $e(\Phi(h_i,h_i) + t_i - \beta(t_i)\kappa)e = c_i$.

Ist n ungerade, so gilt:

$\Phi(h_1 e,h_1 e) = c_1 - e(t_1 - \beta(t_1)\kappa)e$, also:

$\Phi(h_1e,h_1e) + (et_1e + t) - \beta(et_1e + t)\kappa = c_1 + t - \beta(t)\kappa$

und $(c_1 + t - \beta(t)\kappa)(c_{1R}^{-1} - t\kappa + \beta(t)) = 1$. Es folgt:

$$s_{h_1e,C}(x) = x - h_1eC^{-1}b_\theta(h_1e,x) = x - h_1ec_{1R}^{-1}b_\theta(h_1,x)$$
$$= s_{h_1,e,c_1}(x) \text{ für alle } x\varepsilon E.$$

Sei nun n gerade. Es ist: $\Phi(h_1e + h_2e_{12},h_1e + h_2e_{12}) =$

$e\Phi(h_1,h_1)e + e_{21}\Phi(h_2,h_1)e + e\Phi(h_1,h_2)e_{12} + e_{21}\Phi(h_2,h_2)e_{12}$

$= c_1 - e(t_1 - \beta(t_1)\kappa)e + e_{21}b_\theta(h_2,h_1)e - e_{21}\beta(\Phi(h_1,h_2))\kappa e$

$+ e\Phi(h_1,h_2)e_{12} + e_{21}c_2e_{12} - e_{21}(t_2 - \beta(t_2)\kappa)e_{12}$

also mit $T = et_1e + e_{21}t_2e_{12} - e\Phi(h_1,h_2)e_{12} + t$:

$\Phi(h_1e + h_2e_{12},h_1e + h_2e_{12}) + T - \beta(T)\kappa = C$ und:

$C^{-1} = c_{1R}^{-1} - e_{21}c_{2R}^{-1}b_\theta(h_2,h_1)c_{1R}^{-1} + e_{21}c_{2R}^{-1}e_{12} - t\kappa + \beta(t)$.

Damit gilt wegen $eC^{-1}e_{21} = 0$ für alle $x\varepsilon E$:

$$s_{h_1e + h_2e_{12},C}(x) = x - (h_1e + h_2e_{12})C^{-1}b_\theta(h_1e + h_2e_{12},x)$$
$$= x - h_1eC^{-1}eb_\theta(h_1,x) - h_2e_{12}C^{-1}eb_\theta(h_1,x) -$$
$$- h_2e_{12}C^{-1}e_{21}b_\theta(h_2,x)$$
$$= x - h_1c_{1R}^{-1}b_\theta(h_1,x) -$$
$$- h_2(-c_{2R}^{-1}b_\theta(h_2,h_1)c_{1R}^{-1}b_\theta(h_1,x) + c_{2R}^{-1}b_\theta(h_2,x))$$
$$= s_{h_2,e,c_2}(x - h_1ec_{1R}^{-1}b_\theta(h_1,x))$$
$$= s_{h_2,e,c_2}s_{h_1,e,c_1}(x).$$

Im Fall eines Moduls E,b,q haben wir ebenso

$C \varepsilon (q(h_1e) \cap A^*)$ bzw. $C \varepsilon (q(h_1e + h_2e_{12}) \cap A^*)$ und

die Rechnungen verlaufen völlig analog.

§3 Hilfssätze.

Die folgenden Hilfssätze werden wir in den Paragraphen 4 - 6 benötigen. Falls Rechnungen für quadratische Moduln E,θ und E,b,q gleich verlaufen, schreiben wir von nun an nur noch E und verwenden auch im ersten Fall b,q anstelle von b_θ, q_θ. Den ersten Hilfssatz werden wir nur für Schiefkörper oder Summen zweier Schiefkörper brauchen, er gilt jedoch allgemeiner für Ringe A, deren Restklassenringe A/rad(A) nach dem Jacobsonradikal halbeinfach sind. Solche Ringe nennen wir (nicht notwendig kommutative) semilokale Ringe.

3.1 HILFSSATZ Sei E ein quadratischer α,u-Modul über dem semilokalen Ring A, $H \subseteq E$ ein Untermodul und $f,g \in E$ so, daß es $h_o, h_1 \in H$ gibt mit $b(f,h_o) = b(g,h_1) = 1$. Dann gibt es ein $h \in H$ mit $b(f,h) = 1$ und $b(g,h) \in A^*$.

BEWEIS Wegen $b(f,h_o) = 1$ ist h_oA ein freier direkter Summand von H und es gilt $H = h_oA \oplus H_f$, wobei $H_f = \{h \in H \mid b(f,h)=0\}$ ist. Sei $\omega = \{b(g,h_f) \mid h_f \in H_f\}$. ω ist ein Rechtsideal in A und es gilt: $A = b(g,h_o)A + \omega$, da ja für $h_1 \in H$ gilt: $b(g,h_1) = 1$. Daraus folgt: Es gibt eine Einheit in $b(g,h_o) + \omega$. Ein Beweis hierfür steht etwa in -1- Chapter III Prop. 2.8. Es gibt also ein $h_f \in H_f$, so daß für $h_o + h_f$ gilt: $b(g,h_o + h_f) \in A^*$ und es ist $b(f,h_o + h_f) = 1$.

Der folgende Hilfssatz beschäftigt sich mit der Existenz von Einheiten in den Nebenklassen $a + A(\alpha,u)$ für spezielle Ringe A.

3.2 HILFSSATZ Seien A,α,u wie in 2.1 oder 2.2 und sei F_2 der Primkörper mit zwei Elementen. Dann enthält die Nebenklasse $a + A(\alpha,u)$ mit $a \in A$ stets eine Einheit, außer wenn für das in 2.3 konstruierte β,κ einer der folgenden Fälle vorliegt:

3.2.1 $A \cong F_2 \oplus F_2$ und $a + A(\alpha,u) = a + A(\beta,\kappa) = \{(0,1),(1,0)\}$.

3.2.2 $A \cong M_n(R)$, wobei R ein kommutativer Körper, $\beta|_R$ = Identität, $\kappa = 1$, $a \in A(\alpha,u)$ und n ungerade ist.

3.2.3 $A \cong M_2(F_2)$ und $v^{-1}a + A(\beta,\kappa) \in \{\{e_{12},e_{21}\},\{e_{11}+e_{12},e_{11}+e_{21}\},$
$\{e_{12}+e_{22},e_{21}+e_{22}\}\}$.

BEWEIS Wegen $v^{-1}(a + A(\alpha,u)) = v^{-1}a + A(\beta,\kappa)$ enthält $a + A(\alpha,u)$ genau dann Einheiten, wenn $v^{-1}a + A(\beta,\kappa)$ Einheiten besitzt. Indem wir zu $v^{-1}a$ ein geeignetes Element aus $A(\beta,\kappa)$ addieren, können wir erreichen, daß $v^{-1}a + A(\beta,\kappa) = a_o + A(\beta,\kappa)$ ist, wobei a_o eine obere Dreiecksmatrix ist. Ist nun $A \cong M_n(R)$, $R = D \oplus D^{op}$ mit $D \neq F_2$, so enthält $R(\beta,\kappa)$ stets Einheiten von R, wir können also erreichen, daß in der Hauptdiagonalen einer Dreiecksmatrix Einheiten stehen und dann ist diese Matrix c Einheit in $v^{-1}a + A(\beta,\kappa)$, vc also Einheit in $a + A(\alpha,u)$. Ist R ein Körper , $\beta|_R \neq$ Identität oder $\kappa \neq 1$, so kann man ebenso verfahren, es bleiben also nur die Fälle zu untersuchen, daß R ein kommutativer Körper, $\beta|_R$ = Id. und $\kappa = 1$ ist oder daß $R = F_2 \oplus F_2$ ist. Sei zunächst $R = F_2 \oplus F_2$, $A \cong M_n(R)$. Der Fall $n = 1$ ist klar, also ist zu zeigen, daß für $n \geq 2$ $a + A(\beta,\kappa)$ stets eine Einheit enthält. Wir behandeln zunächst die Fälle

$n = 2$ und $n = 3$. R ist kommutativ, also sind die einzigen invertierbaren Matrizen $a \in A$ die mit $\det(a) = 1$, denn 1 ist die einzige Einheit in R. Ist $w \in A^*$, so besitzt $a + A(\beta,\kappa)$ genau dann eine Einheit c, wenn $\beta(w)aw + A(\beta,\kappa)$ eine besitzt, nämlich $\beta(w)cw$. Sei $a + \beta(a) = (d,\beta(d))$ mit $d \in M_n(F_2)$; $\beta(d)$ die zu d transponierte Matrix. Dann gibt es ein $w = (w_1,w_2)$, so daß gilt:

$$\beta(w)(d,\beta(d))w = (\beta(w_2)dw_1,\beta(\beta(w_2)dw_1)) \in \{\sum_{i=1}^{k} e_{ii} \mid 0 \leq k \leq n\},$$

denn man kann w_1,w_2 so wählen, daß $\beta(w_2)dw_1$ diese Gestalt in $M_n(F_2)$ hat. Mit $r = (1,0) \in F_2 \oplus F_2$, $c_1 = re_{11} + (e_{12} + e_{21})$, $c_2 = re_{11} + \beta(r)e_{22} + (e_{12} + e_{21})$ folgt dann für $n = 2$:

$\beta(w)aw + A(\beta,\kappa) \in \{1 + A(\beta,\kappa), c_1 + A(\beta,\kappa), c_2 + A(\beta,\kappa)\}$,

denn es ist $1 + \beta(1) = 0$, $c_1 + \beta(c_1) = e_{11}$, $c_2 + \beta(c_2) = 1$ und $1,c_i \in A^*$ $i=1,2$ und damit ist die Behauptung für $n = 2$ bewiesen.

Ist $n = 3$, so setzen wir:

$$c_1 = \begin{pmatrix} r & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad c_2 = \begin{pmatrix} r & 1 & 0 \\ 1 & \beta(r) & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad c_3 = \begin{pmatrix} r & r & 1 \\ \beta(r) & r & r \\ 1 & \beta(r) & r \end{pmatrix},$$

Es folgt: $1 + \beta(1) = 0$, $c_1 + \beta(c_1) = e_{11}$, $c_2 + \beta(c_2) = e_{11} + e_{22}$, $c_3 + \beta(c_3) = 1$ und $1,c_i \in A^*$, $i=1,2,3$. Demnach gilt für geeignetes w wieder:

$\beta(w)aw + A(\beta,\kappa) \in \{1 + A(\beta,\kappa), c_i + A(\beta,\kappa) \mid i=1,2,3\}$,

also gibt es auch für $n = 3$ für alle $a \in A$ in $a + A(\beta,\kappa)$ eine Einheit.

Sei nun $n \geq 4$, $a_o \in B$ eine obere Dreiecksmatrix. Ist n gerade, so kann man die Matrix entlang der Hauptdiagonalen in 2×2 Kästchen einteilen und a_o mod $A(\beta,\kappa)$ so abändern, daß dort lauter invertierbare Matrizen stehen. Läßt man a_o sonst ungeändert, so ist die so entstandene Matrix invertierbar. Ist $n \geq 5$ ungerade, so wähle man entsprechend eine 3×3 Matrix und sonst lauter 2×2 Matrizen entlang der Hauptdiagonalen und verfahre entsprechend.

Sei nun R ein kommutativer Körper, $\beta|_R = Id.$ und $\kappa = 1$. Ist $A \cong M_n(R)$, so sei V ein n-dimensionaler R-Vektorraum mit Basis $v_1,\ldots,v_n$. Ist $a_o = (a_{ij}) \in a + A(\beta,1) = B_o$ der Vertreter, der obere Dreiecksgestalt hat, so versehen wir V mit einer (gewöhnlichen) quadratischen Form durch $q(v_i) = a_{ii}$ $i=1,..,n$; $b(v_i,v_j) = a_{ij}$ für $1 \leq i < j \leq n$. Wird ein Basiswechsel in V durch die Matrix $w \in A^*$ beschrieben, so folgt $w^T B_o w = w^T a w + A(\beta,1) = B$. Dabei bezeichnet ^{T} das Transponieren in A. Wie man aus der Theorie der quadratischen Formen über Körpern weiß, ist jeder quadratische Vektorraum orthogonale Summe ein- oder zweidimensionaler Unterräume, es gibt also ein $w \in A^*$ so, daß man ein $a_1 = (a_{ij}) \in B$ finden kann mit $a_{ij} \neq 0$ höchstens für die Diagonalelemente a_{ii} und die Elemente $a_{i\,i+1}$ mit i ungerade. Wir müssen also jetzt zeigen, daß, falls a_1 die angegebene Form hat, $a_1 + A(\beta,1) = B$ stets eine Einheit enthält, außer wenn n ungerade und $a_1 \in A(\beta,1)$ ist, oder wenn $R \cong F_2$ ist und die in 3.2.3 angegebenen Ausnahmefälle vorliegen. Dafür gibt es sicher keine invertierbaren Vertreter

in B. Für n = 1 ist nichts zu beweisen und n = 2 kann man unmittelbar nachrechnen. Wir behandeln jetzt noch die Fälle n = 3 und n = 4 gesondert und beweisen dann den Rest durch Induktion nach n.

Sei n = 3, $a_1 = \begin{pmatrix} a_{11} & a_{12} & 0 \\ 0 & a_{22} & 0 \\ 0 & 0 & a_{33} \end{pmatrix}$. Mit a_1 liegen sicher noch folgende Matrizen in B: $a_2 = \begin{pmatrix} a_{11} & a_{12} & 1 \\ 0 & a_{22} & 0 \\ -1 & 0 & a_{33} \end{pmatrix}$,

$a_3 = \begin{pmatrix} a_{11} & a_{12} & 0 \\ 0 & a_{22} & 1 \\ 0 & -1 & a_{33} \end{pmatrix}$, $a_4 = \begin{pmatrix} a_{11} & a_{12} & 1 \\ 0 & a_{22} & 1 \\ -1 & -1 & a_{33} \end{pmatrix}$, $a_5 = \begin{pmatrix} a_{11} & a_{12}+1 & 0 \\ -1 & a_{22} & 0 \\ 0 & 0 & a_{33} \end{pmatrix}$.

Wären alle diese Matrizen nicht invertierbar, so müßten ihre Determinanten alle Null sein. Nun bedeutet $\det(a_1) = 0$: $a_{11}a_{22}a_{33} = 0$. Verwendet man dies in $\det(a_2) = 0$, so folgt $a_{22} = 0$. Damit erhält man aus $\det(a_3) = 0$: $a_{11} = 0$ und wenn man das in $\det(a_4) = 0$ berücksichtigt muß auch $a_{12} = 0$ sein. $\det(a_5) = 0$ liefert nun $a_{33} = 0$, also folgt $a_1 = 0$.

<u>n = 4:</u> Ist $|R| > 2$, so gibt es sicher ein invertierbares Element der Form $\begin{vmatrix} a_{11} & a_{12} & 0 & 0 \\ a_{21} & a_{22} & 0 & 0 \\ 0 & 0 & a_{33} & a_{34} \\ 0 & 0 & a_{43} & a_{44} \end{vmatrix}$ in B. Sei also $R \cong F_2$

und $a_1 = \begin{pmatrix} a_{11} & a_{12} & 0 & 0 \\ 0 & a_{22} & 0 & 0 \\ 0 & 0 & a_{33} & a_{34} \\ 0 & 0 & 0 & a_{44} \end{pmatrix}$.

1.Fall: Es gibt ein $a_{kk} \neq 0$, also $a_{kk} = 1$, $k \in \{1,..,4\}$. Dann können wir durch Umnumerieren der Basiselemente von V $a_{11} = 1$ erreichen. Sei also in a_1 $a_{11} = 1$. Dann liefert der Fall $n = 3$ die Bedingungen $a_{22} = a_{33} = a_{34} = a_{44} = 0$ und dafür ist $e_{11} + a_{12}e_{12} + (e_{13} - e_{31}) + (e_{24} - e_{42}) \in B$ invertierbar.

2.Fall: $a_{ii} = 0$ für $i=1,..,4$. Dann betrachten wir

$$a_2 = \begin{pmatrix} 0 & a_{12} & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & a_{34} \\ -1 & 0 & 0 & 0 \end{pmatrix} \in B \text{ und } a_3 = \begin{pmatrix} 0 & a_{12}+1 & 0 & 1 \\ -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & a_{34} \\ -1 & 0 & 0 & 0 \end{pmatrix} \in B.$$

$\det(a_2) = \det(a_3) = 0$ würde bedeuten: $a_{12}a_{34} = -1$ sowie $(a_{12} + 1)a_{34} = -1$ und das geht nicht.

Sei nun $n \geq 5$ und sei der Satz richtig für alle $m < n$. Wir behandeln die Fälle n gerade und n ungerade gesondert.

<u>n ungerade:</u> Wir nehmen an, es gibt in B kein invertierbares Element und zeigen, daß dann $a \in A(\beta,1)$, also $a_1 = 0$ gilt. Gibt es in a_1 ein $a_{kk} \neq 0$, so können wir wieder annehmen $a_{11} \neq 0$ und da $n - 1$ gerade ist, liefert die Induktionsannahme, daß es in B ein invertierbares Element gibt. Sei also $a_{ii} = 0$ für $i=1,..,n$. Wir betrachten $a_2 = a_1 + (e_{23} - e_{32}) + a_{34}(e_{43} - e_{34})$. Dann erhält man durch Entwickeln nach der 2. und 3. Zeile: $\det(a_2) = \det(a_2')$, wobei man a_2' durch Streichen der 2. und 3. Zeilen und Spalten aus a_2 erhält. Die Induktionsannahme liefert $a_2' = 0$, also folgt $a_1 = a_{12}e_{12}$. Dann gilt für

$$a_3 = a_1 + (e_{13} - e_{31}) + \sum_{j=1}^{\frac{n-1}{2}} (e_{2j\ 2j+1} - e_{2j+1\ 2j})$$

$\det(a_3) = -a_{12}$, also muß auch $a_{12} = 0$ sein.

n gerade: ($n \geq 6$). Es ist zu zeigen, daß in jeder Nebenklasse $a_1 + A(\beta,1) = B$ ein invertierbares Element liegt. Ist $n \geq 8$ oder $|R| > 2$, so folgt das sofort aus dem schon bewiesenen, indem man a_1 entlang der Hauptdiagonalen in ein 4×4 und ein $(n-4) \times (n-4)$ Kästchen, bzw. für $|R| > 2$ in lauter 2×2 Kästchen einteilt und dort findet man ja invertierbare Vertreter. Sei also $n = 6$ und $R \cong F_2$. Gibt es ein $a_{kk} \neq 0$, so sei wieder o.E. $a_{11} \neq 0$ und dann erhält man mit Hilfe der Induktionsannahme, daß nur noch der Fall $a_1 = e_{11} + a_{12}e_{12}$ zu untersuchen bleibt und dafür ist $a_1 + (e_{13} - e_{31}) + (e_{24} - e_{42}) + (e_{56} - e_{65}) \in A^*$. Ist $a_{11} = 0$ für $i=1,..,6$, so entwickle man $a_2 = a_1 + (e_{23} - e_{32}) + a_{34}(e_{43} - e_{34})$ nach der zweiten und dritten Zeile und man erhält wieder $\det(a_2) = \det(a_2')$, wobei a_2' aus a_2 wie oben gewonnen wird. Da es nun in $a_2' + M_4(R)(\beta,1)$ stets ein invertierbares Element gibt, so auch in $a_2 + A(\beta,1) = B$.

3.3 HILFSSATZ Sei A wie in 2.1 oder 2.2 , β,κ wie in 2.3 konstruiert und E ein quadratischer β,κ-Modul. Ferner $f \in E$ und H ein Untermodul von E, der ein Element $h_o \in H$ enthält mit $b(f,h_o) = 1$. Wir setzen $H_f = \{ h \mid h \in H,\ b(f,h) = 0 \}$ und N sei stets ein Modul mit $b(n,n') = 0$ und $q(n) = A(\beta,\kappa)$ für alle $n,n' \in N$.

3.3.1 Ist A ein kommutativer Körper, β = Id., κ = 1, so habe $g \in E$ die folgenden Eigenschaften: $q(g) = q(f)$, $g - f \in H$, $q(g - f) = 0$. Außerdem gebe es ein $h_1 \in H$ mit $b(g,h_1) = 1$. Wir setzen $H_g = \{ h \mid h \in H, b(g,h) = 0 \}$, $H_1 = H_f \cap H_g$ und $S = \{ h \mid h \in H, b(f,h) \in A^*, b(g,h) \in A^* \}$. Ist dann $q(h) = 0$ für alle $h \in S$, so folgt $H \cong N$ für $A \ncong F_2$ und $H \cap H^\perp \cong N$ für $A \cong F_2$.

3.3.2 Ist $A \cong F_2 \oplus F_2$ und gilt $b(h,h) = 1$ für alle $h \in H$ mit $b(f,h) = 1$, so folgt $H_f \cong N$ und $b(h,H_f) = 0$ für alle $h \in H$ mit $b(f,h) = 1$.

3.3.3 Ist $A \cong M_n(R)$ mit n ungerade, R ein kommutativer Körper, $\beta|_R$ = Id. und $\kappa = 1$ und gilt $q(h) = A(\beta,\kappa)$ für alle $h \in H$ mit $b(f,h) = 1$, so ist $\pi(H) \cong N$ falls $R \ncong F_2$ und $\pi(H) \cap \pi(H)^\perp \cong N$ falls $R \cong F_2$. Dabei ist $\pi(h) = he_{11}$ $h \in H$, $\pi(H)^\perp = \{ x \mid x \in \pi(E), b(x,\pi(H)) = 0 \}$.

3.3.4 Ist $A \cong M_2(F_2)$ und gilt $q(h) \in \{\{e_{12},e_{21}\},\{e_{11}+e_{12},e_{11}+e_{21}\}, \{e_{12}+e_{22},e_{21}+e_{22}\}\}$ für alle $h \in H$ mit $b(f,h) = 1$, so gilt ebenfalls $\pi(H) \cap \pi(H)^\perp \cong N$.

BEWEIS Sei A ein kommutativer Körper, β = Id., $\kappa = 1$ und es gelte $q(h) = 0$ für alle $h \in S$. Für beliebige $a \in A$, $x \in H_1$, $y \in S$ ist $xa + y \in S$, also gilt:

$0 = q(xa + y) = q(x)a^2 + b(x,y)a + q(y)$ und damit

3.3.5 $q(x) = b(x,y) = q(y) = 0$ für $A \ncong F_2$

$q(x) + b(x,y) = q(y) = 0$ für $A \cong F_2$. Es ist

$0 = q(g-f) = q(g) - b(g,f) + q(f) = b(g,g) - b(g,f) = b(g,g-f)$, ebenso $b(f,g-f) = 0$, folglich gilt $g - f \in H_1$. 3.3.5 ist also speziell für $x = g - f$ erfüllt und damit gilt stets

$b(g - f,S) = 0$.

Hat nun A mehr als zwei Elemente, so erzeugt S als Vektorraum ganz H, in diesem Fall folgt $b(g - f,H) = 0$ und daraus $H_f = H_g$. Ist $h \varepsilon H$, so gilt entweder $h \varepsilon S$, also $q(h) = 0$ nach Voraussetzung oder $h \varepsilon H_f = H_g = H_1$, also $q(h) = 0$ nach 3.3.5 und es folgt $q(H) = 0$ und daraus $H \cong N$.

Sei jetzt $A \cong F_2$ und $H_o = \{ h \mid h \varepsilon H, b(g - f,h) = 0 \}$. Es gilt $H_o = H_1 \cup S$, denn $h \varepsilon H_o$ bedeutet $b(f,h) = b(g,h)$ und $b(f,h) = b(g,h) = 0$ ist gleichwertig mit $h \varepsilon H_1$, während $b(f,h) = b(g,h) = 1$ heißt: $h \varepsilon S$. Außerdem gilt $H^{\perp} \cap H \subseteq H_o$, also gilt für alle $x \varepsilon H^{\perp} \cap H$ entweder $x \varepsilon H_1$ oder $x \varepsilon S$. Für $x \varepsilon S$ ist $q(x) = 0$ nach Voraussetzung und für $x \varepsilon H_1$ gilt in 3.3.5 $b(x,y) = 0$, da ja außerdem $x \varepsilon H^{\perp}$ ist, also folgt ebenfalls $q(x) = 0$ und damit $H^{\perp} \cap H \cong N$.

Sei nun $A \cong F_2 \oplus F_2$ und $b(h,h) = 1$ für alle $h \varepsilon H$ mit $b(f,h)=1$. Nach Voraussetzung existiert ein solches h und es gilt: $b(f,h + xa) = 1$ für alle $x \varepsilon H_f$, $a \varepsilon A$, also:

$1 = b(h+xa,h+xa) = b(h,h) + b(h,x)a + \beta(b(h,x)a) + \beta(a)b(x,x)a$ oder

3.3.6 $0 = b(h,x)a + \beta(b(h,x)a) + \beta(a)b(x,x)a$. Wäre $b(x,x) = 1$ für ein $x \varepsilon H_f$, so müßte $b(h,x) \notin \{0,1\}$ sein und das ist nicht möglich, da 3.3.6 auch für xa mit $a = b(h,x)$ erfüllt sein muß. Damit ist $b(x,x) = 0$ und $b(h,x)a \varepsilon \{0,1\}$ für alle $x \varepsilon H_f$, $a \varepsilon A$. Gäbe es nun ein $x \varepsilon H_f$ mit $b(h,x) = 1$, so würde mit $a \notin \{0,1\}$ folgen: $b(h,x)a \notin \{0,1\}$, folglich gilt $b(h,H_f) = 0$. Aus $b(x,x) = 0$ für alle $x \varepsilon H_f$ erhält man außer-

dem $b(x,y) \in \{0,1\}$ für alle $x,y \in H_f$ und $b(x,y) = 1$ kann wieder nicht sein, da mit $y \in H_f$, $a \notin \{0,1\}$ auch $ya \in H_f$ ist. Es folgt $H_f \cong N$.

Setzt man in 3.3.1 $g = f$, so folgt 3.3.3 für den Fall $n = 1$. Sei also $n \geq 3$. Es ist $H = h_o A \oplus H_f$ und alle $h \in H$ mit $b(f,h) = 1$ haben die Form $h = h_o + x$ mit $x \in H_f$. Wegen

$$A(\beta,\kappa) = q(h_o + x) = q(h_o) + q(x) + (b(h_o,x) + A(\beta,\kappa))$$

folgt $-b(h_o,x) \in q(x)$ für alle $x \in H_f$. Sei $-b(h_o,x) = (a_{ij})$. Da $-b(h_o, x e_{kl}) \in q(x e_{kl})$ für alle $k,l \in \{1,..,n\}$ gleichwertig mit $\sum_{i=1}^{n} a_{ik} e_{il} \in a_{kk} e_{ll} + A(\beta,\kappa)$ ist, muß $a_{ik} = 0$ für $i \neq l$ sein und für $k = l$ folgt dann ebenfalls $a_{lk} = 0$. Dies gilt für alle k, folglich ist $(a_{ij}) = 0$ und es wird $H = h_o A \perp H_f$ und damit $q(H_f) = A(\beta,\kappa)$. Das alles ergibt $q(H) = A(\beta,\kappa)$ und daraus folgt $q(\pi(H)) = 0$ woraus man sofort $\pi(H) \cong N$ erhält, also erst recht $\pi(H) \cap \pi(H)^{\perp} \cong N$ für $R \cong F_2$.

Sei nun $A \cong M_2(F_2)$. Es ist nach Voraussetzung $b(h,h) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ für alle $h \in H$ mit $b(h,f) = 1$, also folgt wie oben:

$b(x,x) = b(h_o,x) + b(x,h_o)$ für alle $x \in H_f$, denn es ist $1 = -1$.

Sei wieder $b(h_o,x) = (a_{ij})$. Dann ist

$$0 = b(x e_{kl}, x e_{kl}) = b(h_o,x) e_{kl} + e_{lk} b(x,h_o) = \sum_{i=1}^{2} a_{ik}(e_{li} + e_{il})$$

für alle $k,l \in \{1,2\}$ also ebenfalls $(a_{ij}) = 0$ und damit $H = h_o A \perp H_f$ und $b(x,x) = 0$ für alle $x \in H_f$. Aus $b(x,x) = 0$ folgt: $q(x) \in \{A(\beta,\kappa), e_{11} + A(\beta,\kappa), e_{22} + A(\beta,\kappa), 1 + A(\beta,\kappa)\}$.

Annahme: Es gibt ein $x \in H_f$ mit $q(x) \neq A(\beta,\kappa)$. Dann betrachte man xa, wobei a die Gruppe A^* durchläuft. Diese wird erzeugt

von $s = e_{12} + e_{21}$ und $t = e_{11} + s$ und es gilt für $q(x) = e_{11} + A(\beta,\kappa)$: $q(xs) = e_{22} + A(\beta,\kappa)$ und $q(xt) = 1 + A(\beta,\kappa)$. Gibt es also ein $x_o \in H_f$ mit $q(x_o) \notin A(\beta,\kappa)$, so gibt es Elemente $x \in H_f$, so daß $q(x)$ jeden der Werte $e_{11} + A(\beta,\kappa)$. $e_{22} + A(\beta,\kappa)$ und $1 + A(\beta,\kappa)$ annimmt. Außerdem gilt aber: $q(h_o + x) = q(h_o) + q(x)$, also kann man dann ein $x \in H_f$ finden mit $q(h_o + x) = e_{11} + e_{12} + e_{22} + A(\beta,\kappa)$ im Widerspruch zur Voraussetzung. Es ist also $q(H_f) = A(\beta,\kappa)$. Daraus folgt: $b(x,x') + A(\beta,\kappa) = q(x + x') + q(x) + q(x') = A(\beta,\kappa)$ und somit $b(x,x') \in A(\beta,\kappa)$ für alle $x,x' \in H_f$. Gäbe es ein Paar $x,x' \in H_f$ mit $b(x,x') = e_{12} + e_{21}$, so wäre $q(xe_{11} + x'e_{22}) = e_{12} + A(\beta,\kappa) \notin A(\beta,\kappa)$, also gilt $b(x,x') = 0$ für alle $x,x' \in H_f$. Es folgt: $\pi(H_f) \cong N$.

Sei nun $h = h_o a + x \in H$ mit $\pi(h) \in \pi(H)^{\perp}$. Wegen $\pi(h_o), \pi(h_o e_{21}) \in \pi(H)$ ist:

$0 = b(\pi(h_o), \pi(h_o a + x)) = e_{11}(e_{12} + e_{21})ae_{11} = e_{12}ae_{11}$ sowie

$0 = b(\pi(h_o e_{21}), \pi(h_o a + x)) = e_{12}(e_{12} + e_{21})ae_{11} = e_{11}ae_{11}$

also $ae_{11} = 0$ und damit $\pi(h_o a + x) = \pi(x) \in \pi(H_f)$.

Nun ist $\pi(H_f) \cong N$ und damit erst recht $\pi(H) \cap \pi(H)^{\perp} \cong N$.

§4 Witts Satz für Schiefkörper und Summen zweier Schiefkörper.

In diesem Paragraphen sei A entweder ein Schiefkörper mit Involution β oder aber $A = D \oplus D^{op}$, wobei D ein Schiefkörper ist, und es sei wie bisher $\kappa \in \{\pm 1\}$. Im zweiten Fall sei die Involution β wie in 2.3 gegeben durch $\beta((d_1,d_2^{op})) = (d_2,d_1^{op})$. Ist E ein quadratischer β,κ-Modul und F ein Untermodul von E, so definieren wir $l_F: E \to \mathrm{Hom}(F,A) = F^*$ durch $l_F(x)(f) = b(x,f)$ für alle $x \in E, f \in F$. Damit gilt:

4.1 SATZ Seien F,G,H Untermoduln des quadratischen β,κ-Moduls E; F und G seien frei und von endlichem Rang und es gelte:

4.1.1 $l_F(H) = F^*$ und $l_G(H) = G^*$.

Ist R ein kommutativer Körper, β = Id. und κ = 1, so sei:

4.1.2 $H \neq N$ für $A \neq F_2$ und $H \cap H^\perp \neq N$ für $A \neq F_2$.

Weiterhin sei $t: F \to G$ eine Isometrie mit

4.1.3 $t(f) - f \in H$ für alle $f \in F$.

Dann gibt es ein Produkt von Spiegelungen T bezüglich Elementen h_i, c_i mit $h_i \in H$, so daß gilt:

$T(x) - x \in H$ für alle $x \in E$, $T|_F = t$ und $T|_{H^\perp} = \mathrm{Id}$.

BEWEIS Für jede Spiegelung s bezüglich eines Elements $h \in H$ gilt: $s(x) - x \in H$ für alle $x \in E$ und $s|_{H^\perp} = \mathrm{Id}$., wir müssen also zeigen, daß es ein Produkt von solchen Spiegelungen gibt, welches t fortsetzt. Wir führen den Beweis durch Induktion nach dem gemeinsamen Rang r von F und G. Sei r = 1, F = fA, G = gA, g = t(f), also q(f) = q(g). Außerdem setzen wir k = g - f. Wegen 4.1.3 ist $k \in H$.

1. Fall: $b(k,f) \in A^*$. Dann gilt $s_{k,-b(k,f)}(f) = g$ nach 1.10

In den übrigen Fällen wollen wir bis auf eine Ausnahme 1.11 anwenden, wir müssen also ein $h \in H$ finden mit den folgenden Eigenschaften:

4.1.4 Es gibt ein $c \in q(h) \cap A^*$ bzw. $c \in q_\theta(h) \cap A^*$.

Diese beiden Bedingungen sind völlig gleichwertig, wir werden deshalb weiterhin auch im Fall eines quadratischen Moduls E,θ b,q anstelle von b_θ, q_θ schreiben:

4.1.5 Sei wie in 1.11 $h' = k + hc^{-1}b(h,f)$. Dann soll gelten: $b(g,h') \in A^*$.

2.Fall: $b(k,f) = 0$. Es folgt $b(g,k) = 0$. Nach Hilfssatz 3.1 gibt es ein $h_o \in H$ mit $b(f,h_o) = 1$, $b(g,h_o) \in A^*$. Findet man ein $c_o \in q(h_o) \cap A^*$, so kann man 1.11 mit $h = h_o$, $c = c_o$ anwenden. Ein solches c_o existiert sicher, wenn $A = D \oplus D^{op}$ mit $D \neq F_2$ ist oder wenn A ein Schiefkörper ist und $\beta \neq Id.$ oder aber wenn für den Fall, daß $\beta = Id.$, A also kommutativ ist, gilt: $Char(A) \neq 2$ und $\kappa = -1$; denn dann gibt es in jeder Nebenklasse $a + A(\beta,\kappa)$ eine Einheit. Ist A kommutativ, $\beta = Id.$, $\kappa = 1$, so gibt es wegen 4.1.2 und Hilfssatz 3.3.1 ebenfalls ein $h \in H$, so daß 4.1.4 und 4.1.5 erfüllt sind, und ebenso kann man 1.11 im Fall $A \cong F_2 \oplus F_2$ anwenden, wenn es ein $h \in H$ gibt mit $b(f,h) = b(g,h) = 1$ und $b(h,h) = 0$, denn dann können wir $c = 1$ wählen. Es bleibt also nur der Fall: $A \cong F_2 \oplus F_2$ und $b(h,h) = 1$ für alle $h \in H$ mit $b(f,h) = b(g,h) = 1$. Für ein beliebiges solches h gilt dann: $b(k,h) = b(g,h) - b(f,h) = 0$. Sei $a \in A$ mit $a \notin \{0,1\}$. Dann gilt: $a + \beta(a) = 1$, $a\beta(a) = 0$, also $b(ha - k, ha - k) = 0$ und $b(h\beta(a) - k, h\beta(a) - k) = 0$, so

daß die Spiegelungen $s_{ha - k,1}$ und $s_{h\beta(a) - k,1}$ existieren und es wird:

$$s_{h\beta(a) - k,1}s_{ha - k,1}(f) = s_{h\beta(a) - k,1}(f - (ha - k)\beta(a))$$
$$= s_{h\beta(a)-k,1}(f + k\beta(a)) = f + k\beta(a) - (h\beta(a) - k)a =$$
$$= f + k = g.$$

3.Fall: $b(k,f) \neq 0$ und $b(k,f) \notin A^*$. Dieser Fall kommt nur dann vor, wenn A kein Körper ist. Sei zunächst $h \in H$ so gewählt, daß b(f,h) und b(g,h) Einheiten in A sind. Dann ist 4.1.5 gleichwertig mit $b(g,h)^{-1}b(g,k)b(h,f)^{-1} + c^{-1} \in A^*$. Ist $b(g,k) = (d_1, d_2^{op})$, so ist wegen b(g,k) = -b(k,f) entweder $d_1 = 0$ oder $d_2 = 0$, aber nicht beide und $b(g,h)^{-1}b(g,k)b(h,f)^{-1}$ hat die gleiche Gestalt. Ist $|D| \geq 4$, so gibt es in q(h) mindestens zwei Einheiten c,c' und wegen $c - c' \in A(\beta,\kappa)$ hat mindestens eines dieser Elemente, etwa c, die Eigenschaft, daß auch $b(g,h)^{-1}b(g,k)b(h,f)^{-1} + c^{-1} \in A^*$ ist. Ist |D| = 3 und b(h,h) = 0, so gilt dies auch noch und wir können wieder 1.11 anwenden.

Es bleiben also die folgenden Ausnahmefälle:

4.1.6 $A \cong F_2 \oplus F_2$ und

4.1.7 $A \cong F_3 \oplus F_3$ falls $b(h,h) \neq 0$ ist für alle $h \in H$ mit $b(f,h) \in A^*$ und $b(g,h) \in A^*$, und F_3 der Primkörper mit drei Elementen ist.

Zu 4.1.6: Sei $h_o \in H$ mit $b(f,h_o) = b(g,h_o) = 1$. Es folgt $b(k,h_o) = 0$ und $b(k,k) = b(k,g) - b(k,f) = -b(f,k) - b(k,f) = 1$. Gilt für ein h_o außerdem $b(h_o,h_o) = 0$, so sei $h = h_o + kb(g,k)$. Dann ist $b(h,h) = b(h_o,h_o) = 0$ wegen b(k,g)b(g,k) = 0, also existiert $s_{h,1}$. Ferner gilt:

$b(g,h) = 1 + b(g,k)^2 = 1 + b(g,k)$ und

$b(h,f) = 1 + b(k,g)b(k,f)$. Nun ist $b(k,f) = -b(g,k)$ und $b(k,g)b(g,k) = 0$, also $b(h,f) = 1$. Es folgt: $b(g,k) + b(g,h)c^{-1}b(h,f) = b(g,k) + (1 + b(g,k)) = 1$ und man kann für h und c = 1 1.11 anwenden.

Sei nun $b(h_o,h_o) = 1$. Dann ist $b(h,h) = 0$ für $h = h_o + k$ und für $h' = h_o b(f,k) + kb(k,f)$ ebenfalls $b(h',h') = 0$, also existieren $s_{h,1}$ sowie $s_{h',1}$ und es gilt wegen $b(f,k) = 1 + b(k,f)$:

$$s_{h',1}s_{h,1}(f) = s_{h',1}(f - hb(f,k)) = f - hb(f,k) - h' = f + k = g.$$

Zu 4.1.7: Es gilt wieder $b(k,k)\varepsilon A^*$. Sei $h_o\varepsilon H$ mit $b(f,h_o)\varepsilon A^*$, $b(g,h_o)\varepsilon A^*$ und $a = -b(k,k)^{-1}b(k,h_o)$. Dann folgt für $h = h_o + ka$: $b(k,h) = 0$ sowie

$$b(f,h) = b(f,h_o) - b(f,k)b(k,k)^{-1}b(g - f,h_o)$$
$$= (1 + b(f,k)b(k,k)^{-1})b(f,h_o) - b(f,k)b(k,k)^{-1}b(g,h_o).$$

Ist $b(f,k) = (d,0)$ $(d\neq 0)$, so folgt $b(f,k)b(k,k)^{-1} = (-1,0)$, ebenso für $b(f,k) = (0,d)$: $b(f,k)b(k,k)^{-1} = (0,-1)$ und damit erhält man $b(f,h)\varepsilon A^*$. Wegen $b(k,h) = 0$ ist außerdem $b(f,h) = b(g,h)$. Ersetzt man nun noch h durch $hb(f,h)^{-1}$, so kann man also o.E. $h\varepsilon H$ so wählen, daß gilt: $b(f,h) = b(g,h) = 1$ und $b(h,h)\varepsilon A^*$, denn für $b(h,h) = 0$ ist schon alles bewiesen. Wir setzen $h' = h - kb(g,k)$. Dann gilt: $b(g,h') = 1 - b(g,k)^2$ und es ist

$$b(g,k)^2 = \left\{\begin{matrix}(1,0) \text{ für } b(g,k) = (d,0)\\ (0,1) \text{ für } b(g,k) = (0,d)\end{matrix}\right\} (d \neq 0).$$ Ferner

$b(h',f) = \kappa - b(k,g)b(k,f) = \kappa$ sowie $b(h',h') = b(h,h)\varepsilon A^*$, $q(h')$ hat also genau einen Vertreter $c\varepsilon A^*$. Es folgt:

$b(g,k) + b(g,h')c^{-1}b(h',f) = b(g,k) + (1 - b(g,k)^2)c^{-1}\kappa$

$= \left.\begin{matrix}(d,0) + (0,1)c^{-1}\kappa \in A^* \text{ für } b(g,k) = (d,0)\\ (0,d) + (1,0)c^{-1}\kappa \in A^* \text{ für } b(g,k) = (0,d)\end{matrix}\right\}$ also kann

man für h',c 1.11 anwenden.

Damit ist der Induktionsanfang in allen Fällen bewiesen.

Sei nun $r > 1$, $f_1,..,f_r$ eine Basis von F. Nach 4.2.1 gibt es $h_1,..,h_r \in H$ mit $b(h_j,f_i) = \delta_{ij}$ und es folgt mit $V = F^{\perp} \cap H$: $H = \overset{r}{\underset{i=1}{\oplus}} h_i A \oplus V$. Wir wenden die Induktionsannahme auf $F_o = \overset{r-1}{\underset{i=1}{\oplus}} f_i A$ an und erhalten ein Produkt von Spiegelungen T_o mit $T_o|_{F_o} = t$. Es folgt: $t_o(f_i) = T_o^{-1}t(f_i) = f_i$ für i=1,.,r-1, und für alle $f \in F$ ist deshalb

$b(t_o(f) - f,f_i) = b(t_o(f),t_o(f_i)) - b(f,f_i) = 0$ für i=1,.,r-1.

Ferner gilt $T_o(H) = H$ und damit

$t_o(f) - f = T_o^{-1}(t(f) - T_o(f)) = T_o^{-1}((t(f) - f) - (T_o(f) - f)) \in H$,

also sogar $t_o(f) - f \in h_r A \oplus V$.

Wenn wir nun den Induktionsanfang auf $f_r A$ anstelle von F, $t_o f_r A$ anstelle von G und $h_r A \oplus V$ anstelle von H anwenden können, so sind wir fertig, da das so erhaltene Produkt von Spiegelungen $T_1: E \to E$ auf $(h_r A \oplus V)^{\perp}$ die Identität ist, also speziell $T_1 f_i = f_i$ für i=1,..,r-1 liefert. $T_o T_1$ ist dann ein gesuchtes Produkt von Spiegelungen mit dem die Behauptung von Satz 4.1 erfüllt ist.

Sei zunächst $f_1,..,f_r$ eine beliebige Basis von F, $h_1,..,h_r$ wie oben. Dann gilt $b(h_r,f_r) = 1$.

4.1.8 BEH.: Es gibt ein $h_r' \in h_r A \oplus V$ mit $b(h_r',t_o f_r) \in A^*$.

Angenommen, es gelte $b(h_rA + V, t_o(f_r)) = aA$ mit $a \notin A^*$. Wir setzen $x = t_o(f_r) - \sum_{i=1}^{r} f_i b(h_i, t_o(f_r))$ und erhalten

$b(h_j, x) = 0$ für alle $j=1,..,r$ sowie

$b(y,x) = b(y, t_o(f_r)) \in aA$ für alle $y \in V$. Es folgt

$b(H,x) \subseteq aA$ und daraus, da $T_o(H) = H$ ist: $b(H, T_o(x)) \subseteq aA$.

Nun gilt $T_o(x) = t(f_r) - \sum_{i=1}^{r} t(f_i) b(h_i, t_o(f_r))$, also

$T_o(x) = g_r - \sum_{i=1}^{r} g_i b(h_i, t_o(f_r))$. Sei $h \in H$ mit $b(h, g_r) = 1$, $b(h, g_i) = 0$ für $i=1,..,r-1$. Dann folgt:

$1 - b(h_r, t_o(f_r)) = b(h, T_o(x)) \in aA$ und das ist wegen $b(h_r, t_o(f_r)) \in aA$ nicht möglich.

Wir haben also stets $l_{f_rA}(h_rA \oplus V) = (f_rA)^*$,

$l_{t_o(f_r)A}(h_rA \oplus V) = (t_o(f_r)A)^*$.

Nun soll die Basis $f_1,..,f_r$ von F so gewählt werden, daß die Bedingungen unter 4.1.2 für $h_rA \oplus V$ anstelle von H gelten. Ist A ein Körper und $\beta \neq Id.$ oder $\kappa = -1$, oder ist A Summe zweier Körper, so ist nichts zu zeigen. Ist A ein kommutativer Körper, $\beta = Id.$ und $\kappa = 1$, so gibt es wegen 4.1.2 jedenfalls ein $h \in H$ bzw. ein $h \in H^{\perp} \cap H$ mit $q(h) \neq 0$. Nun wähle man $h_r \in H$, $h_r \notin V$ so, daß h in $h_rA \oplus V$ liegt und ergänze h_r zu einer Basis $h_1,..,h_r$ von H mod V . Als Basis von F nehme man dann die zu $h_1,..,h_r$ duale Basis.

§5 Witts Satz für halbeinfache Ringe.

Wie in §2 genügt es, $A = M_n(R)$ mit R wie in 2.1 oder 2.2 und β,κ wie in 2.3 zu betrachten. Sei wie in 2.4 $e = e_{11}$ und $\pi: x \to xe$ ($x \in E$). Wir identifizieren wieder R mit eAe und definieren wie in §4 für einen Untermodul F von E $l_F: E \to F^*$ durch $l_F(x)(f) = b(x,f)$ für alle $x \in E$, $f \in F$. Außerdem schreiben wir auch weiterhin in Moduln E,Θ b,q anstelle von b_Θ, q_Θ. Damit erhält man:

5.1 SATZ Seien F,G,H Untermoduln des quadratischen β,κ-Moduls E; F und G seien frei und von endlichem Rang und es gelte:

5.1.1 $l_F(H) = F^*$ und $l_G(H) = G^*$.

Ist R ein kommutativer Körper, $\beta|_R = \mathrm{Id}$. und $\kappa = 1$, so sei:

5.1.2 $\pi(H) \neq N$ für $A \neq F_2$ und $\pi(H) \cap \pi(H)^\perp \neq N$ für $A \cong F_2$.

Weiterhin sei $t: F \to G$ eine Isometrie mit

5.1.3 $t(f) - f \in H$ für alle $f \in F$.

Dann gibt es ein Produkt T von e-Spiegelungen bezüglich Elementen h_i, c_{iR} mit $h_i \in H$, so daß gilt:

$T(x) - x \in H$ für alle $x \in E$, $T|_F = t$ und $T|_{H^\perp} = \mathrm{Id}$.

BEWEIS Seien $f_1,..,f_r$ eine Basis von F und $h_1,..,h_r \in H$ mit $b(f_i,h_k) = \delta_{ik}$. Es folgt:

$b_R(\pi(f_1e_{j1}),\pi(h_ke_{11})) = b(f_1e_{j1},h_ke_{11}) = \delta_{1k}\delta_{j1} \in R$ und entsprechendes gilt für eine Basis von G. Ist $t_R: \pi(F) \to \pi(G)$ wie in 1.12 definiert durch $t_R(\pi(f)) = \pi(t(f))$ für $f \in F$, so ist t_R eine Isometrie von $\pi(F)$ auf $\pi(G)$ und wir können Satz 4.1 auf $\pi(F),\pi(G),\pi(H),\pi(E),t_R$ anstelle der dortigen F,G,H,E,t anwenden. Wir erhalten also ein Produkt von Spiegelungen T_R des Moduls $\pi(E)$ mit $T_R(x) - x \in \pi(H)$ für alle $x \in \pi(E)$,

$T_R|_{\pi(F)} = t_R$ und $T_R|_{\pi(H)^\perp} = Id$. Nach 1.12 entspricht diesem T_R ein Produkt von e-Spiegelungen T des Moduls E bezüglich Elementen h_i, c_{iR} mit $h_i \in H$, für das gilt:
$\pi(T(x)) = T_R(\pi(x))$ für alle $x \in E$. Da die e-Spiegelungen bezüglich $h_i \in H$ gebildet sind, gilt offensichtlich $T(x) - x \in H$ für alle $x \in E$ und $T|_{H^\perp} = Id$. Außerdem sind t und T A-lineare Abbildungen und es ist für eine Basis $f_1,..,f_r$ von F und $j=1,..,n$:

$$\pi(T(f_i)e_{j1}) = \pi(T(f_ie_{j1})) = T_R(\pi(f_ie_{j1})) = t_R(\pi(f_ie_{j1}))$$
$$= \pi(t(f_ie_{j1})) = \pi(t(f_i)e_{j1}).$$

2.4 liefert nun $T(f_i) = t(f_i)$ für $i=1,..,r$, also $T|_F = t$.

5.2 COROLLAR: Seien F,G,H,E,t wie in Satz 5.1 und es gelte zusätzlich zu den dortigen Voraussetzungen eine der folgenden Bedingungen.

5.2.1 n ist ungerade

5.2.2 R ist kein kommutativer Körper oder $\beta|_R \neq Id$ oder $\kappa \neq 1$.

5.2.3 Es ist $F^\perp \cap H \neq N$ (N wie in 3.3).

Dann gibt es ein Produkt von Spiegelungen T' bezüglich Elementen h_i, c_i mit $h_i \in H$, so daß gilt: $T'(x) - x \in H$ für alle $x \in E$, $T'|_F = t$ und $T'|_{H^\perp} = Id$.

BEWEIS: Ist 5.2.1 erfüllt, so folgt die Behauptung sofort aus 5.1 und 2.5.1. Gilt 5.2.2, so ist $R(\beta,\kappa) \cap R^* \neq \phi$, also existiert $s_{0,c_R,e}$ mit $c_R \in R(\beta,\kappa) \cap R^*$ und das in 5.1 konstruierte T und $Ts_{0,c_R,e}$ leisten dasselbe. Ist also n gerade, so kann man entweder auf T oder auf $Ts_{0,c_R,e}$ 2.5.2 anwenden. Ist neben 5.2.3 auch 5.2.1 oder 5.2.2 erfüllt, so gibt es

nichts mehr zu beweisen. Sei also R ein kommutativer Körper, $\beta|_R = Id$, $\kappa = 1$ und n gerade. Wir wollen zeigen, daß aus $F^{\perp} \cap H \neq N$ folgt $\pi(F)^{\perp} \cap \pi(H) \neq N$. Angenommen, es gilt für alle $h \in F^{\perp} \cap H$ $q(h) = A(\beta,\kappa)$. Dann folgt $b(h,h') \in A(\beta,\kappa)$ für alle $h,h' \in F^{\perp} \cap H$ und $b(h,h') \neq 0$ hätte zur Folge: $b(he_{j1},h'e_{k1}) = e_{1j}b(h,h')e_{k1} \notin A(\beta,\kappa)$ für geeignetes j,k. Es gibt also ein $h \in F^{\perp} \cap H$ mit $q(h) = (a_{ij}) + A(\beta,\kappa)$ und $(a_{ij}) \notin A(\beta,\kappa)$. Gilt für ein $i\varepsilon\{1,..,n\}$ $a_{ii} \neq 0$, so folgt $q(\pi(he_{ii})) \in R^*$. Ist $a_{ii} = 0$ für alle i=1,..,n, so gibt es ein Paar $j,k\varepsilon\{1,..,n\}$ mit $a_{jk} + a_{kj} \neq 0$ und dann folgt $q(\pi(h(e_{j1} + e_{k1}))) \in R^*$. Ist also $F^{\perp} \cap H \neq N$, so gibt es ein $h \in F^{\perp} \cap H$ mit $q(\pi(h)) = c_R \varepsilon R^*$ und damit ist $\pi(F)^{\perp} \cap \pi(H) \neq N$. Da das in 5.1 konstruierte T und $Ts_{h,c_R,e}$ dasselbe leisten erhalten wir mit 2.5.2 die Behauptung.

§6 Witts Satz für semilokale Ringe.

6.1 DEFINITION: Ein Ring A heißt semilokal, wenn A/rad(A) halbeinfach ist. (Siehe auch §3.)

Von nun an ist A stets ein semilokaler Ring, der einen Antiautomorphismus α und ein $u \varepsilon A^*$ besitzt, so daß 1.1 und 1.2 erfüllt sind. α induziert eine Bijektion zwischen der Menge der maximalen Rechtsideale von A und der Menge der maximalen Linksideale von A, also gilt $\alpha(\mathrm{rad}(A)) = \mathrm{rad}(A)$ und daher ist $\bar{\alpha}$: A/rad(A) → A/rad(A) mit $\bar{\alpha}(a + \mathrm{rad}(A)) = \alpha(a) + \mathrm{rad}(A)$ für alle $a \varepsilon A$ ein Antiautomorphismus und $\bar{\alpha}, \bar{u} = u + \mathrm{rad}(A) \varepsilon (A/\mathrm{rad}(A))^*$ erfüllen wieder 1.1 und 1.2. Wie wir in §2 ausgeführt haben, gibt es eine direkte Zerlegung von A/rad(A) in Ringe A_i mit $\bar{\alpha}(A_i) = A_i$ und $A_i \cong M_{n_i}(D_i)$ oder $A_i \cong M_{n_i}(D_i \oplus D_i^{op})$ i=1,..,k; D_i Schiefkörper. Wir setzen $\alpha_i = \bar{\alpha}|_{A_i}$ und $\bar{u} = (u_1,..,u_k)$ mit $u_i \varepsilon A_i^*$. Ist E ein quadratischer α,u-Modul, so zerlegen wir $\bar{E} = E/E\mathrm{rad}(A)$ in der gleichen Weise in $\bar{E} = \overset{k}{\underset{i=1}{\oplus}} E_i$, ebenso $\bar{\theta}$ bzw. $\bar{b}, \bar{q}$.

Sind nun $h_i \varepsilon E_i$, $c_i \varepsilon A_i^*$, i=1,..,k so, daß $s_{h_i,c_i}: E_i \to E_i$ existiert und setzen wir $\bar{h} = (h_1,..,h_k)$, $\bar{c} = (c_1,..,c_k)$, so gilt $\bar{c} \varepsilon (A/\mathrm{rad}(A))^*$. Für ein beliebiges Urbild c von $\bar{c}$ in A folgt $c \varepsilon A^*$ nach dem Nakayama Lemma und $E \to \bar{E}$ ist surjektiv, also gibt es ein Urbild h von $\bar{h}$ in E. Ist $B = \Phi(h,h) + A(\alpha,u)$ (Φ ein Vertreter von θ in $S_\alpha(E)$) bzw. $B = q(h)$ so folgt $\bar{c} \varepsilon B + \mathrm{rad}(A)$, also gibt es ein $c \varepsilon A$, so daß $s_{h,c}: E \to E$ existiert und so daß gilt:

$\overline{s_{h,c}(x)} = s_{\bar{h},\bar{c}}(\bar{x}) = \sum_{i=1}^{k} s_{h_i,c_i}(x_i)$ für alle $x \varepsilon E$. Dieser Liftprozess ist für e-Spiegelungen im Allgemeinen nicht möglich, da ein von Null und Eins verschiedenes Idempotent in A/rad(A) kein Idempotent

als Urbild in A zu haben braucht. Das ist etwa immer dann der Fall, wenn A nullteilerfrei ist.

Sind nun T_i i=1,..,k Produkte von Spiegelungen auf den E_i, so gibt es jedenfalls dann ein Produkt von Spiegelungen T auf E mit $\overline{T(x)} = \sum_{i=1}^{k} T_i(x_i)$, wenn die Anzahl der Spiegelungen in allen T_i gleich ist. Da es außerdem zu jeder Spiegelung eine inverse Spiegelung gibt, sieht man, das dies auch dann noch zu erreichen ist, wenn alle Anzahlen mod(2) gleich sind.

Konstruieren wir für α_i, u_i, A_i die Elemente $v_i \varepsilon A_i^*$ wie in 2.3 und ist $v\varepsilon A$ ein Urbild von $(v_1,..,v_k)$, so gilt wieder $v\varepsilon A^*$. Wir setzen $\beta(a) = v^{-1}\alpha(a)v$ und $\kappa = v^{-1}\alpha(v)u$ und erhalten mit $\overline{\beta} = (\beta_1,..,\beta_k)$, $\overline{\kappa} = (\kappa_1,..,\kappa_k)$, daß $\beta_i\colon A_i \to A_i$ Involutionen sind, die zusammen mit den $\kappa_i \varepsilon \{\pm 1\}$ die Eigenschaften unter 2.3 haben.

Für einen Untermodul F von E sei $l_F\colon E \to F^*$ wieder wie in §4 und §5 definiert. Mit diesen Vorbereitungen wollen wir nun beweisen:

6.2 SATZ: Seien F,G,H Untermoduln des quadratischen α,u-Moduls E; F und G seien frei und von endlichem Rang und es gelte:

6.2.1 $l_F(H) = F^*$ und $l_G(H) = G^*$.

6.2.2 Ist in $A_i = M_{n_i}(R_i)$ R_i ein kommutativer Körper, $\beta_i|_{R_i} = \mathrm{Id}$. und $\kappa_i = 1$, so sei $F_i^{\perp} \cap H_i \neq N$. Ist außerdem $R_i \cong F_2$, so sei noch $H_i \cap H_i^{\perp} \neq N$. (N hat die gleiche Bedeutung wie in 3.3)

6.2.3 Für $A_i \cong F_2 \oplus F_2$ sei $H_i \neq h_o A \perp N$, wobei $b_i(h_o,h_o) = 1$ ist. Weiterhin sei $t\colon F \to G$ eine Isometrie mit

6.2.4 $t(f) - f \in H$ für alle $f\varepsilon F$.

Dann gibt es ein Produkt T von Spiegelungen bezüglich Elementen $h^j \varepsilon H$, $c^j \varepsilon A^*$, so daß gilt:

$T(x) - x \in H$ für alle $x\varepsilon E$, $T|_F = t$ und $T|_{H^{\perp}} = \mathrm{Id}$.

BEWEIS: Ersetzen wir Θ bzw. b,q durch $v^{-1}\Theta$, bzw. $v^{-1}b, v^{-1}q$ mit dem oben konstruierten v, so folgt mit 1.13, daß wir den Satz nur für quadratische β,κ-Moduln zu beweisen brauchen. β ist also ein Antiautomorphismus, so daß alle β_i i=1,..,k Involutionen sind und κ ist so, daß für alle i=1,..,k gilt: $\kappa_i \in \{\pm 1\}$. Wir zeigen zunächst, daß wir auf alle F_i, G_i, H_i, t_i 5.2 mit T_i anstelle des dortigen T anwenden können. Das geht sicher immer dann, wenn für kein i gilt:

6.2.5 $A_i = M_{n_i}(R_i)$, R_i ein kommutativer Körper, $\beta_i|_{R_i} = Id.$ und $\kappa_i = 1$. Gilt 6.2.5, so folgt aus $H_i \neq N$ $\pi(H_i) \neq N$, wie im Beweis von 5.2.3 gezeigt wurde, und $F_i^{\perp} \cap H_i \neq N$ ergibt $H_i \neq N$, also ist dann wegen 6.2.2 5.1.2 und 5.2.3 erfüllt und damit gelten auch hier die Voraussetzungen von 5.2. Wegen 6.2.2 gibt es überdies stets ein $h_i \in F_i^{\perp} \cap H_i$, für das ein $c_i \in A_i^*$ existiert, mit dem man s_{h_i,c_i} bilden kann und $T_i s_{h_i,c_i}$ leistet dasselbe wie T_i. (Gilt nicht 6.2.5, so wähle man etwa $h_i = 0$.) Wir können also annehmen, daß alle T_i Produkte einer von i unabhängigen Anzahl von Spiegelungen sind, also gibt es ein $T_o: E \to E$ mit $\overline{T_o(x)} = \sum_{i=1}^{k} T_i(x_i)$ für alle $x \in E$, $\overline{x} = (x_1,..,x_k)$. Es folgt mit $t_o = T_o^{-1}t$: $t_o(f) - f \in Erad(A)$ für alle $f \in F$ und t_o ist eine Isometrie $F \to t_o F$, die wieder alle Voraussetzungen von 6.2 erfüllt. Wenn wir nun t_o durch ein Produkt von Spiegelungen T_1 bezüglich Elementen aus H zu einer Isometrie von E fortsetzen können, so sind wir fertig, da dann $T = T_o T_1$ ein gesuchtes Produkt von Spiegelungen ist. Wir brauchen also 6.2 nur noch für den Fall zu beweisen, daß zusätzlich

gilt: $t(f) - f \in E\,\mathrm{rad}(A)$ für alle $f \in F$. Wir führen den Beweis durch Induktion nach $r = \mathrm{Rang}_A(F)$.

$r = 1$: Sei $F = fA$, $t(f) = g$, also $b(k,f) = b(g-f,f) \in \mathrm{rad}(A)$ und $h \in H$ mit $b(f,h) \in A^*$. Dann gilt auch $b(g,h) \in A^*$. Wir wollen 1.11 anwenden, müssen also ein $h \in H$ mit $b(f,h) \in A^*$ finden, für das $\Phi(h,h) + A(\beta,\kappa)$ bzw. $q(h)$ eine Einheit c besitzt. Dazu wählen wir Elemente h_i mit $b_i(f_i,h_i) = 1$ und mit $(\Phi_i(h_i,h_i) + A_i(\beta_i,\kappa_i)) \cap A_i^* =: C_i \neq \phi$ bzw. $q_i(h_i) \cap A_i^* =: C_i \neq \phi$. Wegen 6.2.2 sowie Hilfssatz 3.2, 3.3.3 und 3.3.4 gibt es ein solches h_i sicher immer dann, wenn $A_i \neq F_2 \oplus F_2$ ist und in diesem Fall folgt die Existenz aus 6.2.3 in Verbindung mit 3.3.2. Wir merken noch an, daß wir hier nur brauchen, daß es ein h_i gibt mit $b_i(f_i,h_i) = 1$ und $b_i(h_i,h_i) = 0$. Dies werden wir am Schluß des Beweises benötigen. Sei nun h ein Urbild von $(h_1,..,h_k)$ in H und $c \in \Phi(h,h) + A(\beta,\kappa)$ bzw. $c \in q(h)$ mit $\bar{c} = (c_1,..,c_k)$, $c_i \in C_i$. Ein solches c gibt es, da $\overline{A(\beta,\kappa)} = \overset{k}{\underset{i=1}{\oplus}} A_i(\beta_i,\kappa_i)$ ist. Es folgt $c \in A^*$. Wir können also für h,c 1.11 anwenden und erhalten ein Produkt zweier Spiegelungen s mit $s(f) = g$.

Sei nun $r > 1$, $f^1,..,f^r$ eine Basis von F. Wir wollen wie in Satz 4.1 verfahren und wählen wie dort $h^1,..,h^r \in H$ mit $b(h^j,f^i) = \delta_{ij}$. Die Induktionsannahme liefert uns dann ein Produkt von Spiegelungen T_2 an Elementen aus H mit $T_2(f^i) = t(f^i)$ für $i=1,..,r-1$ und es gilt mit $t_2 = T_2^{-1}t$, $V = F^{\perp} \cap H$ wie in 4.1 für alle $f \in F$: $t_2(f) - f \in h^rA \oplus V$. Da 4.1.8 für beliebige Ringe A gilt ist 6.2.1 für f^rA anstelle von F, $t_2(f^r)A$ anstelle von G und $h^rA \oplus V$ anstelle von H erfüllt und mit dem Obigen auch 6.2.4. Wir wollen

jetzt die Basis $f^1,..,f^r$ von F so wählen, daß $h^rA \oplus V$ anstelle von H auch 6.2.2 erfüllt; und daß für $A_i \cong F_2 \oplus F_2$ gilt: $b_i(h_i^r,h_i^r) = 0$ sowie $b_i(f_i^r,h_i^r) = 1$ für ein geeignetes $f_i^r \varepsilon F_i$. Im letzteren Fall gibt es wegen 6.2.3 solche h_i^r für alle Basiselemente f_i^r von F, ebenso gilt wegen $V_i \neq N$ im Fall 6.2.5 stets $h_i^rA_i \oplus V_i \neq N$. Ist $A_i \cong M_{n_i}(F_2)$, so verfahren wir wie im Beweis von 4.1. Für die übrigen i wählen wir h_i^r so, daß es ein $f_i^r \varepsilon F_i$ gibt mit $b_i(f_i^r,h_i^r) = 1$. Ist h_r dann ein Urbild von $(h_1^r,..,h_k^r)$, so hat $h^rA \oplus V$ die gewünschten Eigenschaften. Wir ergänzen nun h^r zu einer Basis von H mod(V) und wählen in F die dazu duale Basis. Auf f^rA, $t_2(f^r)A$, $h^rA \oplus V$ können wir nun den Induktionsanfang anwenden, denn das Produkt von Spiegelungen T_3 bezüglich Elementen aus $h^rA \oplus V$, durch das wir wieder $T_3^{-1}t_2(f^r)-f^r \varepsilon Erad(A)$ erreichen, ändert nichts an den Voraussetzungen. Es gibt also wieder ein Produkt zweier Spiegelungen T_4 bezüglich Elementen aus $h^rA \oplus V$ mit $T_4(f^r) = T_3^{-1}t_2(f^r)$. Da sowohl $T_3(f^i) = f^i$ als auch $T_4(f^i) = f^i$ für i=1,..,r-1 gilt ist $T = T_2T_3T_4$ ein gesuchtes Produkt von Spiegelungen. $T(x) - x \in H$ und $T|_{H^\perp} = Id.$ ist natürlich auch erfüllt.

Wollen wir die Isometrie t nicht notwendig durch ein Produkt von Spiegelungen fortsetzen, so können wir einige Einschränkungen über F, G und H weglassen, denn es gilt:

6.3 HAUPTSATZ: Sei A ein semilokaler Ring, $\alpha: A \to A$ ein Antiautomorphismus, der zusammen mit $u \varepsilon A^*$ 1.1 und 1.2 erfüllt und E ein quadratischer α,u-Modul. Seien F, G und H Untermoduln von E mit F und G endlich erzeugt und projektiv und

es gelte:

6.3.1 $l_F(H) = F^*$ und $l_G(H) = G^*$.

6.3.2 Ist $A_i = M_{n_i}(R_i)$, R_i ein kommutativer Körper, $\beta_i|_{R_i} = Id.$ und $\kappa_i = 1$, so sei $F\frac{|}{i} \cap H_i \neq N$. Dabei ist β,κ wie in 6.2. Sei $t: F \to G$ eine Isometrie mit

6.3.3 $t(f) - f \in H$ für alle $f \in F$.

Dann gibt es eine Isometrie $T: E \to E$, die t fortsetzt und für die gilt: $T(x) - x \in H$ für alle $x \in E$ und $T|_{H\perp} = Id.$

BEWEIS: Es genügt wieder, den Satz für quadratische β,κ-Moduln zu beweisen, wobei β,κ wie in 6.2 sind. Wir nehmen zunächst an, daß F,G frei und von endlichem Rang sind. Sind außerdem die zusätzlichen Bedingungen aus 6.2 erfüllt, so folgt 6.3 aus 6.2. Ist das nicht der Fall, so gibt es mindestens ein A_i mit

6.3.4 $A_i \cong M_{n_i}(F_2)$, $H\frac{|}{i} \cap H_i \cong N$ oder

6.3.5 $A_i \cong F_2 \oplus F_2$, $H_i \cong h_iA_i \perp N$ mit $b_i(h_i,h_i) = 1$

Wir ersetzen nun E durch $E' = E \perp (yA \oplus zA)$ mit $\Phi(y,z) = 1$, $\Phi(y,y) = \Phi(z,y) = 0$ und $\Phi(z,z) = a$ für einen Vertreter Φ von 0 bzw. $b(y,z) = 1$, $q(y) = A(\beta,\kappa)$ und $q(z) = a + A(\beta,\kappa)$. Dabei ist $a \in A$ so zu wählen, daß für $\bar{a} = (a_1,..,a_k)$ gilt: $0 \neq a_i \neq 1$ falls 6.3.5 vorliegt, sonst $a_i = 0$. In E' betrachten wir nun $F' = F \perp yA$, $G' = G \perp yA$, $H' = H \perp (y + z)A$ und $t' = t \perp Id_{yA}$. Es gilt $b(y,y + z) = 1$, also ist $l_{F'}(H') = F'^*$ und $l_{G'}(H') = G'^*$ erfüllt. Außerdem gilt $q(y + z) = 1 + a + A(\beta,\kappa)$, also $q_i(y_i + z_i) = \beta_i(a_i) + A_i(\beta_i,1)$ falls 6.3.5 vorliegt und $q_i(y_i + z_i) = 1 + A_i(\beta_i,\kappa_i)$ sonst.

Ist $A_i \cong M_{n_i}(F_2)$, so liegt $y_i + z_i$ in $H_i' \cap H_i'^{\perp}$, also gilt $H_i' \cap H_i'^{\perp} \not\subseteq N$. Ist $A_i \cong F_2 \oplus F_2$ und liegt 6.3.5 nicht vor, so gilt $b_i(y_i + z_i, y_i + z_i) = 0$, sonst $b_i(y_i + z_i, y_i + z_i) = 1$, also in jedem Fall $H_i' \not\subseteq h_i A \perp N$ mit $b_i(h_i, h_i) = 1$. Außerdem gilt $F^{\perp} \cap H \subseteq F'^{\perp} \cap H'$, demnach ist für $A_i = M_{n_i}(R_i)$, R_i ein kommutativer Körper, $\beta_i|_{R_i} = \mathrm{Id}$ und $\kappa_i = 1 : F_i'^{\perp} \cap H_i' \not\subseteq N$. Da für H_i' nicht die Ausnahmefälle 6.2.2 und 6.2.3 auftreten, können wir 6.2 anwenden und erhalten ein Produkt von Spiegelungen T' bezüglich Elementen aus H' für das gilt: $T'|_F = t$, $T'(y) = y$, $T'(x) - x \in H'$ für alle $x \in E'$ sowie $T'|_{H'^{\perp}} = \mathrm{Id}$. Wir wollen $T = T'|_E$ setzen, müssen also noch zeigen: $T'(E) \subseteq E$, $T'(x) - x \in H$ für alle $x \in E$ und $T'|_{H^{\perp} \cap E} = \mathrm{Id}$. Wegen $T'(x) - x \in H'$ gilt für alle $x \in E$: $T'(x) = x + h_x + (y + z)a_x$ mit $h_x \in H$, $a_x \in A$. Es folgt: $0 = b(y,x) = b(T'(y), T'(x)) = b(y, x + h_x + (y + z)a_x) = a_x$. Außerdem gilt $H^{\perp} \cap E \subseteq H'^{\perp}$, da $b(E, y + z) = 0$ ist und damit haben wir 6.3 für den Fall freier Moduln F und G bewiesen.

Seien nun F und G projektiv und endlich erzeugt. Dann gibt es einen Modul F', so daß $F \oplus F'$ frei und von endlichem Rang ist. Sei F'^* der Dualmodul von F'. $F' \oplus F'^*$ machen wir zu einem quadratischen Modul durch: $\Phi(\lambda, f') = \lambda(f')$, $\Phi(f_1', f_2') = \Phi(\lambda, \lambda') = \Phi(f', \lambda) = 0$ bzw. $q(f') = q(\lambda) = A(\beta, \kappa)$ $b(\lambda, f') = 1$ für alle $f', f_1', f_1' \in F'$, $\lambda, \lambda' \in F'^*$. Wir ersetzen nun E durch $E \perp (F' \oplus F'^*)$, F durch $F \perp F'$, G durch $G \perp F'$, H durch $H \perp F'^*$ und t durch $t \perp \mathrm{Id}_{F'}$. $t \perp \mathrm{Id}_{F'} : F \perp F' \to G \perp F'$ ist eine Isometrie, also ist auch $G \perp F'$ frei. Ferner gilt

$1_{F \perp F'}(H \perp F'^*) = (F \perp F')^*$ und $1_{G \perp F'}(H \perp F'^*) = (G \perp F')^*$ nach Konstruktion sowie $(F \perp F')^{\perp} \cap (H \perp F'^*) = F^{\perp} \cap H$, also bleibt 6.3.2 erfüllt und wir erhalten mit dem schon Bewiesenen eine Isometrie $T'\colon E \perp (F' \oplus F'^*) \to E \perp (F' \oplus F'^*)$ mit $T'|_F = t$, $T'|_{F'} = \mathrm{Id}$, $T'(x) - x \in H \perp F'^*$ für alle $x \in E \perp (F' \oplus F'^*)$ und $T'|_{(H \perp F'^*)^{\perp}} = \mathrm{Id}$. Es ist $F'^* \subseteq (H \perp F'^*)^{\perp}$, also gilt auch $T'|_{F'^*} = \mathrm{Id}$ und damit folgt $T'(E) \subset E$, denn es ist $E = (F' \oplus F'^*)^{\perp}$. $T = T'|_E$ ist also eine gesuchte Isometrie.

L I T E R A T U R V E R Z E I C H N I S

-1- H.BASS: Algebraic K-Theory, Benjamin 1968

-2- N.BOURBAKI: Modules et anneaux semi-simples;
Algèbre , Chap. 8 Hermann 1958

-3- A.M.McEVETT: Forms over Semisimple Algebras with Involution,
J.Algebra 12, 1969, 105-113.

-4- M.KNEBUSCH: Isometrien über semilokalen Ringen,
Math.Z. 108, 1969, 255-268

-5- M.KNESER: Witts Satz für quadratische Formen über lokalen Ringen,
Nachrichten des Akademie der Wissenschaften, Gött. 1972

-6- C.T.C.WALL: On the axiomatic foundations of the theory of
Hermitian forms, Proc.Camb.Phil.Soc. 67, 1970, 243-250

Lebenslauf

Am 10. Januar 1944 wurde ich in Wien als Sohn des damaligen Werfttechnikers Johann Reiter und dessen Ehefrau Erika, geb. Dargatz, geboren und im Herbst 1950 eingeschult. Im September 1951 übersiedelte ich mit meiner Mutter nach Wilhelmshaven, wo ich Ostern 1954 in die Max-Planck-Schule, das math.-naturwissenschaftliche Gymnasium der Stadt aufgenommen wurde. Im Februar 1964 legte ich dort die Reifeprüfung ab.

Im Sommersemester 1964 begann ich mit dem Mathematikstudium an der Universität Göttingen. Nach der Vordiplomprüfung am 10.5.1966 studierte ich hauptsächlich unter der Leitung von Herrn Prof. Dr. M. Kneser. Von ihm erhielt ich auch das Thema meiner Diplomarbeit und am 24.10.1968 bestand ich die Hauptdiplomprüfung.

Seit Dezember 1968 vertrete ich von einer kurzen Unterbrechung abgesehen die Stelle eines wiss. Assistenten; zuerst in Göttingen und seit Oktober 1970 in Mainz.

Meine akademischen Lehrer waren vor allem die Herren Professoren: M.Deuring, B.Huppert, M.Kneser, G.Lüders, G.Lyra und A.Pfister.